VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

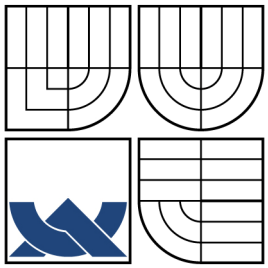
FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF MANAGEMENT

MODEL INCIDENT MANAGEMENTU V DIALOGOVÉM ROZHRANÍ E-COMMERCE

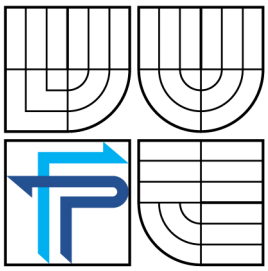
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Bc. VLASTIMIL ŠIMČÍK
AUTHOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF MANAGEMENT

MODEL INCIDENT MANAGEMENTU V DIALOGOVÉM ROZHRANÍ E-COMMERCE

INCIDENT MANAGEMENT MODEL IN DIALOG INTERFACE OF E-COMMERCE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. VLASTIMIL ŠIMČÍK
AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. JIŘÍ DVOŘÁK, DrSc.
SUPERVISOR

BRNO 2011

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/2011
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Šimčík Vlastimil, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Model Incident managementu v dialogovém rozhraní e-commerce

v anglickém jazyce:

Incident management Model in the Dialog Interface E-commerce

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DOSEDĚL,T. Počítačová bezpečnost a ochrana dat. 1. vydání. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1
KOTLER, P. Marketing management. 1. vydání, Praha: Grada, 2007. 788 s. ISBN 978-80-247-1359-5
PUŽMANOVÁ, R. Moderní komunikační sítě od A do Z. 2. aktualizované vydání. Brno: Computer Presss, 2006. 430s. ISBN 80-251-1278-0
SODOMKA,P. Informační systémy v podnikové praxi. 2.aktualizované vydání. Brno: Computer Press, 2010. 499s. ISBN 978-80-251-2878-7
VOŘÍŠEK, J. Principy a modely řízení podnikové informatiky. 1. vydání. Praha: Oeconomica, 2008. 446 s. ISBN 978-80-245-1440-6

Vedoucí diplomové práce: prof. Ing. Jiří Dvořák, DrSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2010/2011.

L.S.

_____	_____
PhDr. Martina Rašticová, Ph.D.	doc. RNDr. Anna Putnová, Ph.D., MBA
Ředitel ústavu	Děkan fakulty

V Brně, dne 22.05.2011

Abstrakt

Tato práce pojednává o zavedení Incident managementu jako o jednom z možných prostředků pro minimalizaci rizik a ztrát vzniklých organizaci výpadky v jejich infrastruktuře, či nedostupností jejich „business critical“ aplikací. Zaměřena je především na organizace zaměřené na elektronické obchodování.

Klíčová slova

ITSM, ITIL, Availability, Incident management, SLA

Abstract

This essay deal with implementation of the Incident management as one of the possible means to minimize risks and losses arising from failures in the organization’s infrastructure and inaccessibility of their "business-critical" applications. It focuses primarily on the organization focused on electronic commerce.

Key words

ITSM, ITIL, Availability, Incident management, Service Level Agreement

Bibliografická citace VŠKP dle ČSN ISO 690

ŠIMČÍK, V. *Model Incident managementu v dialogovém rozhraní e-commerce.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 86 s. Vedoucí bakalářské práce Prof. Ing. Jiří Dvořák, DrSC.

.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb. O právu autorském a o právech souvisejících s právem autorským).

V Brně, dne 26. května 2011 . . . . . .

podpis

Poděkování

Na tomto místě bych rád poděkoval zejména mé rodině a mým přátelům, kteří mne podporovali při mých studiích, a i když to občas nebylo lehké, vždy mi dokázali podat pomocnou ruku a podpořit mne. Dále bych rád poděkoval profesorskému sboru a vedení fakulty za příjemné prostředí a atmosféru, kterou dokázali vytvořit během výuky a že nám studentům vždy dokázali vyjít vstříc a podat pomocnou ruku v nesnázích.

Obsah:

Úvod

Jako téma své diplomové práce jsem si zvolil implementaci Incident managementu v organizacích zabývajících se E-commercí, i když základní myšlenka Incident managementu jako takového je shodná pro implementaci v jakékoliv organizaci, ať už se zaobírá čímkoliv.

V současné době se E-commerce stala běžnou součástí denního života firem i jednotlivců a do budoucnosti se bude tato „zavislost“ stále více prohlubovat, neboť tzv. elektronická cesta, se svojí schopností přenosu dat rychlostí jinak nedosažitelnou, nám již v současné době naznačuje možnosti, které nelze dobudoucna nejen nevyužít, ale přímo i naznačuje cesty, kterými je nutno se zabývat. Ať už to bude přímo o elektronických trasnakcích, nebo o dalších možnostech elektronických médii, jako různé průzkumy trhu, reklamní činnost, statistické možnosti a spoustu jiných. Tento rychlý rozmach a defacto všudypřítomnost E-commerce však na druhou stranu přináší nová, dosud nepoznaná rizika a úskalí, se kterými je zapotřebí bojovat. Někdy je tento boj úspěšný více jindy méně, jak se říká, na každou akci následuje reakce, takže v současné době je to věčný boj mezi organizacemi zajiš´tujícími bezpečnost při pohybu v elektronickém porstředí a druhou stranou, která se neustále snaží nalézt mezery, chyby či metody jak tyto ochrany obejít a buď na ně poukázat (lepší varianta) či je nějakým způsobem zneužít (horší varianta). Spolu s těmito novými variantami ale stále koexistují i stará a již dobře známá rizika spojená se spolehlivostí technických komponent, či zásahu přírodních živlů, které se dají jen těžko ovlivnit. Protože již z teorie řizení rizik víme, že nikdy nejdou všechna rizika úplně odstranit, nebo pouze za podmínek, kdy finální řešení přináší defacto nemožnost provozovat jakoukoliv činnost, proto zde přichází ke slovu vhodné metody na mitigaci rizik. A jednou z nejúčinnějších metod je implementace efektivního Incident mamagementu, který nám nejenom umožňuje co nejefektivněji a v co možná nejkratším čase vrátit stav systémů na původní úroveň, ale díky poznatkům z průběhu těchto incidentů taktéž přináší významné poznatky do preventivnich opatření a tímto plní i funkci proaktivního článku v celeém řetězu řízení rizik.

V první teoretické části se budu věnovat základům, ze kterých budu posléze vycházet při tvorbě mého vlastního návrhu, to znamená, že přinesu pohled na metody

řízení rizik, jejich dělení, hodnocení, způsoby klasifikace apod. Dále poskytnu přehled základních systémů ITSM, které se v dnešní době používají a drží trend v moderních společnostech zabývajících se informačními technologiemi. Zde v části věnované systému ITIL také podrobněji rozvinu kapitolu Incident managementu. V druhé teoretické části následuje analýza současného stavu, kde se budu nejprve věnovat tématice analýze rizik v prostředí E-Commerce, a to hlavně z hlediska identifikace a ohodnocení rizik, jaké jsou typické druhy ohrožení v prostředí E-Commerce, jaké jsou v tomto směru poslední trendy, jaké jsou dopady takovýchto bezpečnostních incidentů či jak tvořit ve firmách bezpečnostní rámce. Následovat bude analýza současné situace ohledně implementace Incident managementu ve firmách, jaké jsou jeho hlavní zásady, jaké jsou hlavní výzvy pro Incident management, jak se buduje proaktivní Incident management, či jaká jsou hlavní pravidla pro jeho implementaci.

V části praktické se potom pokusím nastínit vytvoření modelu Incident management desku pro podporu organizace zabývající se (nejen) E-Commercí. Tato část bude vytvořena formou projektu. Model Incident desku by měl zaručovat plně hodnotný servis v 12h směnném modelu s pokrytím 24/7/365 a samozřejmě by měl poskytnout nástroj k naplnění cílů, které budou v projektu stanoveny. Součastí projektu bude jak analýza rizik projektu, tak kompletní WBS s vyhledáním critické cesty za pomoci CPM. Na závěr vyhodnotím přínosy projektu a uzavřu práci pohledem na celkovou problematiku v současném světě.

1. Vymezení problému a cíle

1.1 Vymezení problému

Účelem této práce je analyzovat rizika ohrožující organizace zabývající se eletronickým obchodováním z hlediska jejich „daily business“ aktivit (E2E, B2B, B2C, infrastruktura) a na tomto základě navrhnout řešení na zvýšení availability zmíněných komponent a snížení ekonomických ztrát způsobených jejich výpadkem.

1.2 Vymezení pojmu „dialogové rozhraní“ pro účely mé práce

Dialogové rozhraní pro účel mé práce je definováno jako jakékoliv rozhraní mezi uživatelem systému a jeho provozovatelem, může tedy zahrnovat různé aplikace, služby, komunikační kanály apod.

1.3 Cíl práce

Cílem mé práce je návrh modelu Incident managementu pro organizace zabývající se elektronickým obchodováním, jakožto jednoho ze základních prvků zabezpečujících snižení rizik a ztrát způsobených výpadkem „bussiness crtitcal“ aplikací a infrastruktury.

1.4 Užitý metodologický aparát

Při zpracování své diplomové práce budu využívat logicko systematickou metodu pro nalezení optimálního modelu.

Logicko systematická metoda na nalezení optimálního modelu

Postup v případě metody:

- analyzuji současnou situaci, znázorním základní prvky
- k základním prvkům přidám nové poznatky a názory získané studiem a diskusemi a analyzuji je
- následně na základě předchozích analýz zformuluji závěry
- po zanalyzování a formulaci všech nových závěrů, a přidání všech nových poznatků, dojdu k hledanému cíli.

Vymezení způsobů získávání autentických a objektivních informací a jejich zdrojů

- osobní pracovní zkušenosti
- tématická literatura
- internet
- materiály institucí, které tvoří, používají nebo se zabývají EPS a průzkumy veřejného mínění
- komunikace s uživateli

2. Teoretická východiska práce

V této části se budu věnovat teoretickým východiskům vhodným pro moji samostatnou část práce. Jsou to zejména analýza, ohodnocení a management rizik a systémy ITSM které určijí dnešní trendy při správě procesů v moderních společnostech. Zde pak samostatně vyzdvihnu úlohu Incident mamagementu a jeho postavení v rámci systému ITIL. V příloze na konci práce je potom možno nálézt minimum z historie obchodu a E-Commerce jako takové.

2.1 Anlýza rizik

Analýza rizik je nedílnou součástí při rozhodování pro zavedení Incident managementu, proto se v této části mé práci chci alespoň zevrubně dotknout tohoto tématu. Zabývá se převážně odhalováním a pochopením rizik a následně poskytuje podklady pro rozhodnutí o nutnosti zabývat se určenými riziky a doporučuje nejvhodnější a nákladově efektivní strategii zvládání rizik. Analýza rizik obsahuje odhalení zdrojů rizik, jejich příznivých a nepříznivých následků a možností, že se tyto následky přihodí. Mohou být identifikovány faktory, které ovlivňují následky a jejich pravděpodobnosti. Rizika se analyzují spojením následků a jejich pravděpodobností. Posledním bodem je navržení opatření na eliminaci či snížení dopadu rizika. Blíže se k analýze rizik význačných pro prostředí E-Commerce vrátím v části rozboru současného stavu.

2.1.1 Definice rizika

Riziko můžeme obecně definovat jako nebezpečí vzniku určité ztráty.
Finanční teorie definuje riziko jako volatilitu (kolísavost) finanční veličiny (hodnoty portfolia, zisku, atd.) okolo očekávané hodnoty v důsledku změn celé řady parametrů. Z této definice vyplývá, že jak negativní, tak ale i pozitivní odchylky jsou považovány za zdroje rizika. (3, 4, 16)

Další definice rizika:

- Pravděpodobnost či možnost vzniku ztráty, obecněnezdaru
- Variabilita možných výsledkůnebo nejistota jejich dosažení

- Odchýlení skutečných a očekávaných výsledků
- Pravděpodobnost jakéhokoliv výsledku, odlišného od výsledku očekávaného
- Nebezpečí chybného rozhodnutí
- Možnost vzniku ztráty nebo zisku, atd.

Riziko je třeba hodnotit ze dvou stránek, a to z:

- pozitivní stránky – naděje vyššího zisku, naděje vyššího úspěchu,
- negativní stránky – nebezpečí horších hospodářských výsledků.

My se budeme dále zabývat převážně rizikem negativním.
Ztráty mohou vzniknout prostřednictvím kombinace dvou faktorů

- volatility finančních proměnných, ovlivňujících míru rizika
- celkové angažovanosti k těmto zdrojům rizika

2.1.2 Klasifikace rizik

Rizika jako taková můžeme rozdělit do 3 základních skupin:

- kritické riziko: veškerá ohrožení, jehož potenciální ztráty jsou takového řádu, že vyústí v bankrot firmy,
- důležité riziko: takové ohrožení, jehož potenciální ztráty nevyústí v bankrot, avšak další provoz bude vyžadovat, aby si firma vypůjčila,
- běžné riziko: takové ohrožení, jehož potenciální ztráty mohou být pokryty stávajícími aktivy firmy nebo běžným příjmem, aniž by došlo k nepatřičnému finančnímu tlaku.

Další dělění rizik je dle místa působení rizik:

- dynamické riziko – zdroj se nachází ve firmě či okolí
- statické riziko – zdroj mimo ekonomiku – příroda, lidský faktor

Dle chrakteru rizika:

- spekulativní – riziko může působit jak v kladném, tak záporném charakteru
- čisté – pouze záporný charakter rizika

Dle rozsahu působení:

- celková – široký dopad na obyvatelstvo, politické či národně ekonomické události
- dílčí – ovlivňují pouze individuální prvky

2.1.3 Metody snižování rizik

Metody snižování rizik nám napomáhají vyrovnat se, eliminovat, či snížit dopady rizika na činnost firmy. Základní rozdělní rizik a metod na jejich snížení uvádí následující tabulka:

Pravděpodobnost / **Tvrdost**	**Vysoka**	**Nízká**
Vysoká	**Vyhnutí se riziku, redukce**	**Pojištění**
Nízká	**Retence a redukce**	**Retence**

Tabulka 1: Metody snižování rizik vzhledem k jejich dopadu

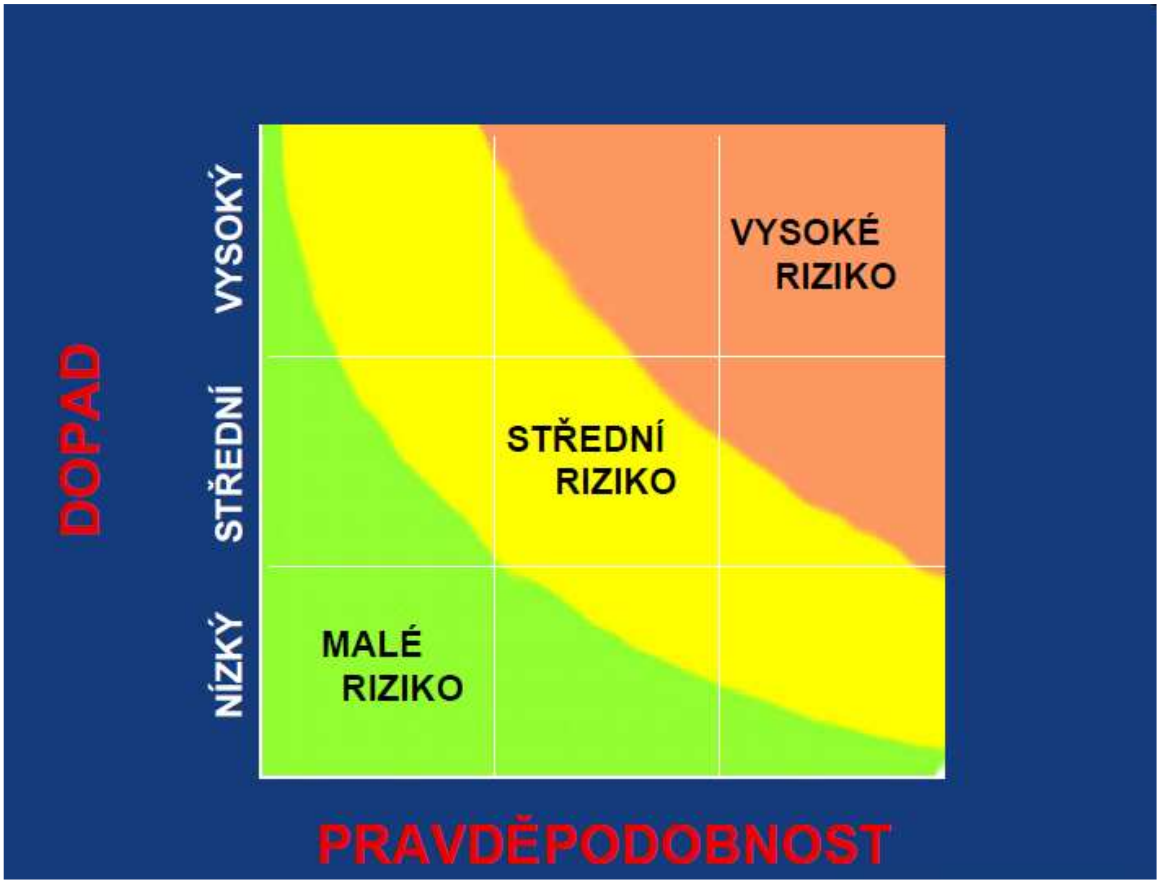
Metody snižování rizik:

- Přesun rizika na jiné podnikatelské subjekty (transfer rizika),
- Uzavírání dlouhodobých kupních smluv na dodávky surovin a komponent za předem stanovené pevné ceny (eliminace cenových rizik),
- Uzavírání komisionářských smluv, které zajišťují prodej výrobků v cizí obchodní síti,
- Uzavírání obchodních smluv, podmiňujících odběr minimálního množství produktů,

- Přesun problému technické inovace výroby na spolupracující firmu,
- Termínové obchody (hedging),
- Leasing (přenos finančního rizika podnikatele, které je spojeno s vlastnictvím daného zařízení, na leasing firmu),
- Odkup pohledávek – faktoring, forfaiting,
- Akreditivy,
- Frančíza, atd.

2.1.4 Mapa rizik

Mapa rizik nám umožňuje graficky znázornit rizika spojená s projektem a zaměřit se převážně na tzv. klíčová rizika, která se nacházejí v růžové oblasti „Vysoké riziko“ na následujícím obrázku. Dále hodnotíme rizika na hlavní (žlutý segment) a běžná (zelený segment). (4, 16)



Obrázek 1: Mapa rizik - zdroj: Ernst&Young

Při tvorbě mapy rizik určitého projektu se postupuje následujícím způsobem:

1. tvorba tabulky rizik s ohodnocením jejich dopadů a pravděpodobnosti výskytu
2. zanesení těchto rizik dle údajů z tabulky od grafické podoby

2.2 Systémy ITSM a řízení procesů IT

V této kapitole pohovoříme o všech moderních a významných sytémech ITSM a sytémech řízení procesů IT, které se v dnešní době podílejí na chodu a udávají takt v celosvětovém IT businessu. Tyto systémy, přestože mnohdy na první pohled vypadají, že se zabývají stejnými věcmi, se většinou používají ve společné symbióze a vzájemně se doplňují, neboť buď nahlížejí na stejnou (či podobnou) problematiku řízení IT z rozdílných úhlů či úrovní, nebo se zabývají procesy obsahově jinými, přestože neméně důležitými (LEAN, SIX SIGMA). V mé práci tuto pasáž uvádím zejména z důvodu, že Incident management, který je defacto zakládním námětem mé práce je součástí právě těchto systému a proto je dobré poskytnou o tomto ucelený obraz.

2.2.1 ITIL

ITIL – je zkratka pro „Information Technology Infrastructure Library“. Je to sada doporučení, praktik pro poskytování IT služeb jehož začátky se datují do roku 1980, kdy na základě aktivity britské státní telekomunikačni a informační agentury vzniká základ prvního ITIL – první sada doporučení pro řízení podniků zabývajících se IT. Doporučeni jsou založena a kopírují tzv. Demigův cyklus (P-D-C-A). Na těchto základech se v roc 1989 oběvuje první verze ITIL, která obsahuje cca. 30 tzv. knih, které je věnují jednotlivým oblastem IT. V roce 2000 přichází na svět ITIL verze 2., který přináší kosolidaci 30 knih do 8mi logických knih a stává se tak přehledným a mnohem jednoduššeji implementovatelným. Největšími knihami jsou kapitoly zabývající se Service management a to knihy Service support a Service delivery. Incident management je zde definovám jako jedna z 5ti součástí knihy service support. V roce 2007 přichází na svět ITIL v.3, který v 5ti knihách poskytuje ucelený pohled na lifecykle celého SM procesu se zaměřením na business model poskytovaný zákazníkovi. Vtomto je také největší rozdíl od předchozí verze, kde tento důraz byl kladen na jednotlivé aspekty jenotlivých služeb SM. Pokud jde o definování ITIL jako takového, jedná se o ucelený rámec pokrývající kompletní životní cyklus IT služeb a jeho podporu v rámci celého IT oddělení. Prostřednictvím procesů postavených na

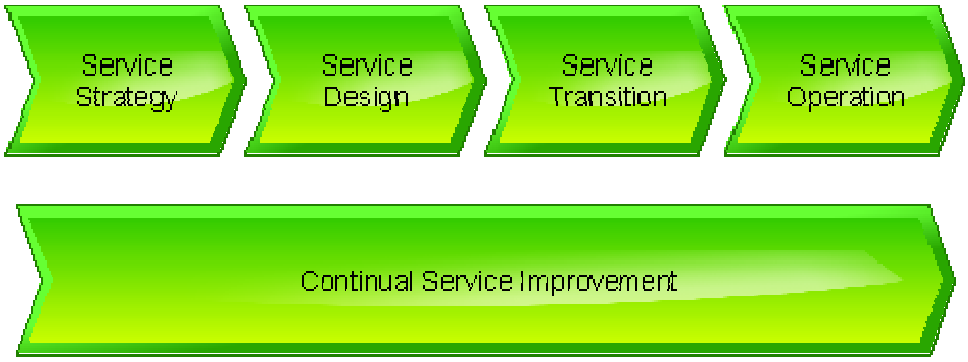
ITILu je možné zprůhlednit činnost IT oddělení a tím dosáhnout přínosů, jako například:

- Sladění činnosti IT oddělení s potřebami celé organizace,
- jasné definování IT služeb poskytovaných IT oddělením,
- zajištění dostupnosti IT služeb dle požadavků celé organizace,
- dosažení finančních úspor prostřednictvím zefektivnění činnosti IT oddělení a optimalizace IT infrastruktury.(7, 8, 25)

Životní cyklus IT služeb v ITIL v3 se skládá z 5 fází:

- Service strategy (Strategie služeb)
- Service design (Návrh služeb)
- Service transition (Implementace služeb)
- Service operation (Provoz služeb)
- Continual service improvement (Neustálé zlepšování služeb) (25)

Jednotlivé fáze na sebe navazují a zároveň si předávají zpětnou vazbu. Tím dochází k uzavření celého cyklu, který navazuje na životní cyklus obchodního procesu/produktu.



Obrázek 2: Cyklus ITIL (zdroj: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/ITIL.aspx)

Incident management v rámci ITIL

Úvod

Jako téměř všechny podniky a organizace spoléhají na své systémy informační technologie (IT), v případě, že nefungují správně, může to mít obrovský dopad na celou činnost firmy. Incident management je proces pro řešení problémů v oblasti IT a může mít zásadní vliv v případě že věci nejdou tak jak by měli. Proto by měl být Incident management zahrnut do rámci komplexního a promyšleného business kontinuity plánu. Bez vhodného řízení, může incident stát vaší firmy obrovské sumy peněz k dosažení obnovení původního stavu. To může zahrnovat ztrátu příjmů, právní náklady, nebo poškození produktů, zařízení, pověsti a nebo dokonce zdraví zaměstnanců. Tato kapitola obsahuje úvod do Incident management a koncepci politiky Incident managementu..

Využití Incident managementu

Cílem Incident management je k obnovení normálního provozu co nejdříve po neočekávané události s negativními následky.
Incident management v organizaci může:

• Analyzovat události, které by mohly ohrozit vaší organizace nebo obchod,
• identifikovat nebezpečí, když k nim dojde,
• pomůže obnovit normální provoz co nejdříve a zároveň minimalizuje dopad na obchodní operace,
• poskytuje zpětnou vazbu po incidentu, pro zajištění zlepšení procesu. ()

Mnoho organizací má vyhrazený samostatný Incident Response Team nebo Incident management Team.

Proč je Incident management tak důležitý? Efektivní Incident management může ušetřit vaší firmě peníze a zajistit, že vaše podnikání může pokračovat bez přerušení i když se vaše systémy informační technologie (IT) staly dočasně nedostupnými. Dobrý Incident

management systém může vést ke snížení:

• Ztráty příjmů,

• soudních výloh,

• škod na výrobcích, zařízení nebo provozech,

• poškození značky a pověsti.

Všechny organizace mohou těžit ze systému Incident managementu. Tyto události nejsou tak časté, ale můžou být velmi škodlivé, nejsou-li úspěšně zvládnuty.(18)

Definování incidentu

Information Technology Infrastructure Library (ITIL) definuje rámec incidentu jako "jakoukoliv událost, která není součástí standardního provozování určité služby a která způsobuje, nebo může způsobit přerušení nebo snížení kvality těchto služeb".Tato definice se může lišit mezi jednotlivými organizacemi, ale je to obecně událost, která ohrožuje jak obchodních aktivity společnosti, tak může způsobit i nedodržení zákonných požadavků nebo zásad společnosti.(7, 9, 18)

Běžné akcí vedoucí k takovému incidentu zahrnují:

• Násilné útoky na své IT systémy, např. počítačové viry nebo hacking,

• požáry,

• povodně,

• krádeže.

Bez účinného Incident managementu může incident rychle ovlivní zbytek vašeho podnikání. To následně může způsobit dopad v těchto oblastech:

• Obchodní operace,

• informační bezpečnost,

• IT systémy,

• zaměstnanci nebo zákazníci,

• další důležité podnikové funkce.

Zajištění včasné a vhodné reakce

Organizace by měla mít jasné pokyny v podobě metodiky Incident managementu. Jedná se o soubor postupů, které pomohou určit příčinu incidentu a následně zaručí obnovení

normálního stavu v co nejkratší době.
Prvním krokem je vždy kvalifikovat události a zjistit, jak to zapadá do konkrétního Incident management systému. Pokud je událost velkého dopadu pak tato může být kvalifikována jako krizová a bude vyžadovat další zdroje a pravděpodobně i zapojení eterních subjektů – vzniká tzv. „Major incident“. (7, 9, 18)

Připrava firmy na incident

Jakým nejlepším způsobem reagovat na mimořádné události závisí na požadavcích konkrétní organizace. Na místě je zde se zamyslet na tím, jaké požadavky bude mít podnik ohledně reakce na vzniklé události v určité situaci a na základě tohoto pak vytvořit metodiku Incident managementu.

Aby bylo možné úspěšně řešit veškeré problémy, které se mohou vyskytnout, je důležité mít veškeré části systému Incident managementu již v provozu před tím, než incident nastane. Například byste měli:
• shromažďovat kontaktní údaje zaměstnanců, kteří budou pravděpodobně zapotřebí, a zaměstnanců, kteří mohou být povoláni na jako back-up
• vytvořit konkrétní telefonní číslo pro použití během mimořádných událostí - můžete použít mobilní nebo bezplatné telefonní číslo – tzv. MoD – manager on duty číslo.
• zřídit speciální e-mailový účet pro použití při mimořádných událostech – důležité převážne v situacích, kdy se standardní emailová adresa stane nedostupná.
• vyhnout se pokud možno používání alternativ, jako jsou různé textové zprávy či záznamníky, pro udržení informovanosti všech zainteresovaných složek – pokud možno používat spolehlivější a časově více kritické formy komunikace. (7, 9, 18)

Také by měl existovat seznam pohotovostních čísel s kontakty na externí pracovníky / organizace a mít tento seznam k dispozici pro své zaměstnance. Součástí tohoto seznamu by měla být například tato čísla:
• Policie (místní a národní)
• pojišťovny,
• advokáty,
• obchodní sdružení.

• čísla vašich hlavních klientů
• místní samosprávy
Tento seznam by měl také existovat ve formě off-site pro případ poškození sídla organizace.

Reakce na incident

Incident management politika by měla být přizpůsobena potřebám organizace, ale existují určitá pravidla, která by měli být součástí všech IM politik bez rozdílu. Mít jasný postup, který by měl být dodržován, pomáhá zaměstnancům, aby jednaly rychle a s minimálním množstvím chyb. (7, 9, 18)

Většina procesů Incident managementu jsou tvořeny z pěti hlavních kroků:
• Kontrola
• kategorizace,
• protiopatření,
• vyhodnocení,
• uzavření. (18)

Rychlost, s jakou budete reagovat, je životně důležitá k zabránění dalším škodám s dopadem na organizaci. Nicméně, měli byste si být vědomi toho, že při pokusu o odstranění problému je snadné způsobit další škody.
Je důležité být opatrný při řízení jakékoliv události, ke které dochází v rámci podnikání.
Měli byste:
• Se ujistit, že nezničíte veškeré důkazy týkající se incidentu
• zachovat místo události, tak jak bylo a zabránit přístupu k podezřelému zařízení,
• záznamenat veškeré okolností spolu s podepsaným svědectvím svědků, a s časem a datem kdy k události došlo,
• zachovat všechny zdroje důkazů o incidentu.
Měli byste vždy jednat metodicky a jasně komunikovat s pracovníky, informovat je o jakékoli události a udržovat povědomí o současné situaci.

Zásady k zapamatování:

• Informujte své zákazníky co nejdříve, jestliže incident ovlivňuje vaše poskytování služeb jim,

• zaměřte se na uvedení maximálního množství informací o incidentu v záznamu o něm,

• neupravovat jakýmkoliv způsobem místo činu, je-li zde podezření na trestný čin,

• vytvořit „forenzní“ back-up příslušných údajů nebo systémů.

Činnosti po ukončení incidentu

Incident management je stejně důležitý poté, co problém byl vyřešen, jako během incidentu sámotném. Je velmi důležité posoudit škodu, která byla způsobena a navrhnout, jak můžeme podobné události zabránit opakovat se v budoucnu.(18)

Měli byste:

• Určit plný rozsah poškození nebo proniknutí,

• uskutečnit rozhovory se svědky nebo zainteresovanými stranami,

• shromaždit důležité podklady a informace,

• otestovat všechny systémy na stupeň informační bezpečnosti,

• určení bezpečnostních mezer a rizik - detailní operační přezkoumání osvědčených postupů, procesních toků, systémů a dat a vyhodnocování rizik,

• shromažďovat záznamy o pracovnících - např. oddělení lidských zdrojů.

Kontrola metodik

Jakmile je opět obnoven normální provoz, je důležité přezkoumat své Incident management metodiky.

V případě technického incidentu – jako např. externí „hacking“ – možná budete muset provést upravy na zvýšení zabezpeční, jako například:

• Technická vylepšení – vylepšení používaných systémů,

• instalace nových opravných patchů - program pro aktualizaci software, obvykle opravuje zjištěné chyby, bezpečnostní díry a problémy,

• provést recenzi konfigurací - analýzy místních nastavení a mechanismy kontroly přístupu s cílem identifikovat potenciální slabá místa v zabezpečení nebo oblasti pro zlepšení,

• posílení ochrany sítě – zajišit, aby antivirové ochrany, firewally a další bezpečnostní

složky sítě byly up-to-date,
• revize na zjištění možných průniků - kontrola všech nových, neznámých, případně podivných interních nebo externích přístupů do počítačové sítě.

Musíte také uplatnit zpětnou vazbu ze svých zjištění a aplikovat je následně do:
• firemní politiky
• politiky lidských zdrojů a vzdělávání zaměstnanců
• smluvních záležitostí – např. externích dodavatelů
• outsourcingových dohod

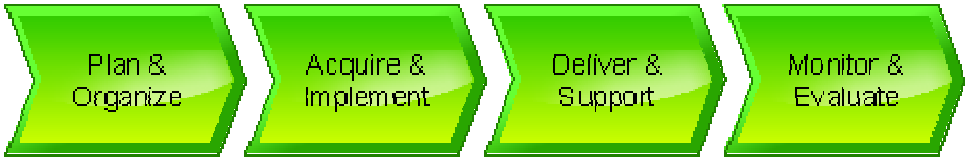
2.2.2 COBIT

COBIT – je zkratka pro „Control Objectives for Information and related Technology“. Jeho znik se datuje do roku 1996. Během doby prošel několika releasy, poslední z nich je verze 4.1 z roku 2007. Vznikl jako rámec pro řízení a kontrolu IT procesů. Úkolem COBITu je zkoumat, vytvářet, publikovat a propagovat aktuální mezinárodně uznávanou sadu cílů pro každodenní měření procesů. Umožňuje vedení společnosti (lidem bez IT backgroundu) řídit a kontrolovat IT v souladu s cíli společnosti. COBIT je postaven na předpokladu, že IT poskytuje informace potřebné pro dosažení cílů společnosti prostřednictvím IT procesů využívajících IT zdroje. (1, 20)

Procesy se skládají z jednotlivých aktivit a jsou rozděleny do 4 domén:

- Plan & Organize (Plánování a organizace)
- Acquire & Implement (Osvojení a implementace)
- Deliver & Support (Poskytování a podpora)
- Monitor & Evaluate (Monitorování a vyhodnocování)

Jednotlivé domény na sebe navazují a zároveň si předávají zpětnou vazbu. Tím dochází k uzavření celého cyklu, který navazuje na životní cyklus obchodního procesu/produktu.



Obrázek 3: Cyklus CobiT (zdroj: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/CobiT.aspx)

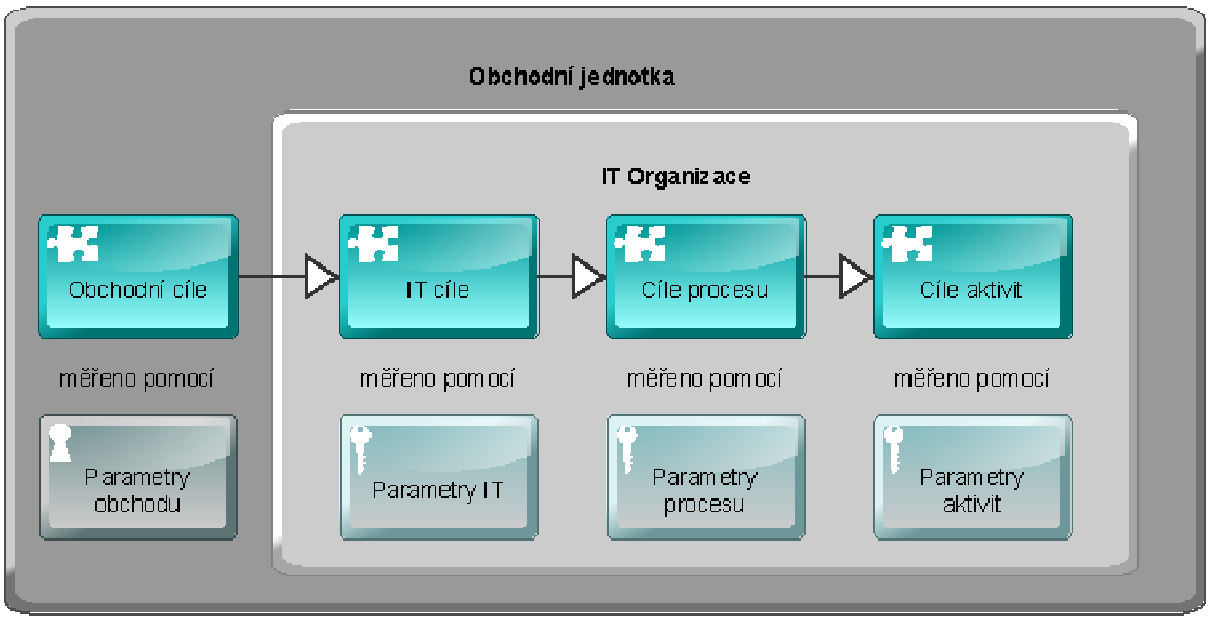
Zdroje jsou rozděleny do 4 oblastí:

- Aplikace
- Informace
- Infrastruktura
- Lidé

Kvalita poskytovaných informací se pak posuzuje podle následujících kritérií:

- Efektivnost
- Výkonnost
- Důvěryhodnost
- Integrita
- Dostupnost
- Soulad
- Spolehlivost

Tato rozdělení pomáhají definovat výkonnostní parametry pro IT organizaci v souladu s obchodními cíli. V rámci COBITu jsou tedy definovány 4 domény s 34 procesy obsahující 318 výkonnostních parametrů. (20)



Obrázek 4: Definování výkonnostních parametrů pro IT organizaci v souladu s obchodními cíli (zdroj: : http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/CobiT.aspx)

2.2.3 CMMI

Datum vzniku CMMI (Capability Maturity Model Integration) se datuje v roce 1987, kdy Software Engineering Institue při Mellonově univerzitě vydal první model pro softwarové procesy. Model byl postupně vyvíjen a v roce 1990 dostal poprvé označení CMM – Capability Maturity Model. V roce 1995 byl vydán podobný model pro návrhy technologických celků S-CMM – System Engineering CMM. Tím vedle sebe existovali 2 velmi podobné standardy, které se nakonec sloučili do jednotného modelu CMMI. Slůvko „integration“ znační právě ono sloučení několika standardů. (21)

CMMI je metoda zlepšování procesů, která poskytuje základní elementy efektivních procesů pro zlepšení vašich procesů. Pomáhá integrovat jednotlivá oddělení, nastavovat cíle a priority pro zlepšování jednotlivých procesů. V současnosti se CMMI skládá ze tří modelů:

- CMMI pro vývoj služeb
- CMMI pro poskytování služeb
- CMMI pro nákup služeb

CMMI přistupuje k procesům ze dvou pohledů, "průběžný" a "úrovňový". V případě "průběžného" přistupu se zaměřuje na specifický proces a jeho sladění s obchodními cíli. V případě "úrovňového" přístupu poskytuje standardní sadu zlepšení pro dosažení další "úrovně" zralosti. (21)

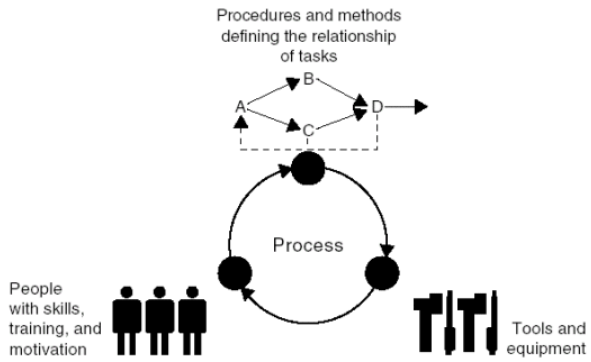
Pro "průběžný" přístup existují 4 oblasti:

- Řízení procesů
- Řízení projektů
- Návrh a realizace
- Podpůrné procesy

V případě "úrovní" existuje 5 úrovní zralosti procesů:

- Počáteční
- Řízená
- Definovaná
- Kvalitativně řízená
- Optimalizovaná

CMMI, stejně jako ostatní metody, pokrývá všechny 3 oblasti, které musí být v souladu, aby implementace byla úspěšná:



Obrázek 5: Model CMMI (zdroj: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/CMMI.aspx**)**

Model je svým určením velice blízký známému modelu ISO 9000:2001, avšak s několika zásadními rozdíly. ISO 9000:2001 je aplikán na firmy z nejrůznějších oborů bez jakékoliv vyhraněnosti na určitou oblast. Oproti tomu je CMMI určem převážně pro vývojové teamy. Podobně je tomu is podrobnosí jedotlivých systému. Zatímco ISO 9000:2001 je spíše formátu obecného s definováním pouze cílů, model CMMI jde do podrobností ať už při definicich činností, či pracovních výstupů. (21)

2.2.4 LEAN

Lean jako metodika pro štíhlou výrobu byla vyvnuta po 2.světové válce firmou Toyota jako TPS – Toyota Production System. Tato metoda se vznačuje řízením se podle hesla „Náš zákazník, náš pán“ a snaží se uspokojovat zákazníkovy požadavky tím, že bude vyrábět opravdu jen to, co zákazník požaduje, s minimálními náklady, bez ztráty kvality a v co nejkratší době. Následně tímto dochází k minimalizaci plýtvání. (26)

Lean jako takový je přístup/metoda napomáhající zlepšovat pracovní postupy a eliminovat zbytečnou ztrátu času, peněz a materiálu. Lean se snaží zajistit, aby se správné věci dostaly na správné místo ve správném čase. Tato metoda se uplatňuje jak ve výrobě, tak i v kanceláři. (26)

Cílem použití přístupu Lean je:

- Eliminovat plýtvání
- Minimalizovat zásoby
- Zrychlit pracovní postupy
- Reagovat na požadavky zákazníků
- Splnit požadavky zákazníků
- Zamezit předělávání
- Zainteresovat pracovníky
- Zavést kulturu zlepšování

To vede k základním principům Lean:

- Definovat hodnotu z pohledu zákazníka

- Zdokumentovat tvorbu hodnoty
- Zajistit nepřerušovaný výrobní postup
- Produkovat pouze, je-li to požadováno
- Všechno je možné zlepšit

Na základě těchto principů jsou pak rozděleny jednotlivé nástroje metody Lean. To napomáhá k jednoduché volbě, který nástroj a kdy použít. Je nutné si ale vždy uvědomit, že prvotní je určení problému, a teprve potom zvolení nástroje. Ne naopak. Nezaměňujte prostředek (nástroj) a cíl (vyřešení problému, ne použití nástroje) !!!(26)

2.2.5 SIX SIGMA

Six Sigma je metoda původně vyvinutá společností Motorola za účelem identifikace a odstranění příčin defektů a chyb v procesech. Později byla dále spracována do současné podoby společnostmi GE a Honeywell.

Six Sigma je metoda určená ke zvyšování kvality procesů a tím i celých firem. Tato metoda je postavena na identifikaci řešení problému pomocí shromážděných a vyhodnocených dat. Zakladní charakeristika metody Six Sigma je rozhodování na základě faktů, ne pocitů. (28)

V rámci metody existuje několik modelů. Nejběžnějšími modely jsou DMAIC pro existující procesy/produkty a DFSS pro nové procesy/produkty. Model DMAIC umožňuje definovat problém, měřit a analyzovat data, implementovat zvolené řešení a následně kontrolovat, zda přineslo očekávané výsledky. Model DMAIC se skládá z kroků:

- Define (Definuj)
- Measure (Měř)
- Analyze (Analyzuj)
- Implement (Implementuj)
- Control (Kontroluj)

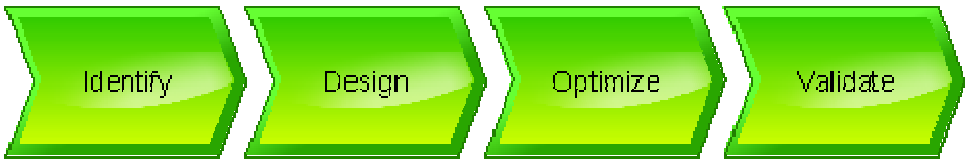
Kroky na sebe navazují a ukončení poslední fáze může iniciovat spuštění nového cyklu:

Obrázek 6: Cyklus DMAIC (zdroj: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/SixSigma.aspx)

Model DFSS umožňuje identifikovat potřeby zákazníka, navrhnout způsob jejich uspokojení, optimalizovat zaváděné řešení a vyhodnotit, zda toto řešení skutečně uspokojilo tyto potřeby. Model DFSS se skládá z kroků:

- Identify (Identifikuj)
- Design (Navrhni)
- Optimize (Optimalizuj)
- Validate (Ověř)

Kroky na sebe navazují a ukončení poslední fáze tohoto cyklu může iniciovat spuštění nového cyklu, ale tentokrát DMAIC:



Obrázek 7: Cyklus DFSS (zdroj: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/SixSigma.aspx)

Metoda Six Sigma je nástroj, který v konečném důsledku umožňuje:

- Efektivní využívání zdrojů
- Uspokojení skutečných potřeb zákazníků
- Snížení skladových zásob
- Snížení chybovosti a s tím spojených nákladů
- Zrychlení procesů
- Eliminaci přístupu pokus/omyl a s tím spojených nákladů

S implementací a používáním metody Six Sigma jsou samozřejmě spojené určité náklady (jako s každou metodou). Je proto potřeba vždy zvažovat, kdy se implementace, či využití, vyplatí a kdy je potřeba použít jednodušší metody/nástroje, např. Lean. (21)

3. Analýza problému a současné situace

3.1 Management rizik v prostředí E-Commerce

Jak jsem již předeslal v kapitole Ananlýza rizik, budu se zde věnovat podrobněji analýze rizik typických pro prostředí E-Commerce, jakožto výchozí bodu pro zpracování metod na snižovaní či eliminace rizik a tímto i rozhodným bodem pro úvahy nad zavedením, či nezavedením Incident managementu.

3.1.1 Úvod

Bariéry vstupu na e-commerce jsou poměrně nízké, ale nové příležitosti mohou být doprovázeny novými riziky. Posouzením rizik se rozumí vytvoření seznamu všech rizik které mohou během provozu nastat, a přiřadit jim různý stupeň závažnosti na základě jejich dopadu na provoz a pravděpodobnosti výskytu. Řízením rizik se rozumí prioritizace těchto rizik a formulování politiky a postupů k jejich eliminaci, či jejich zmírnění. Každý podnik zabývající se E-Commerci může mít prospěch z vyhodnocení rizika jejich systému, i když menší podniky nemusí provádět právě všechny techniky analýzi a některé sofistikovanější techniky, které budou popsány dále, mohou být vynechány. V této části práce se pokusím vysvětluje rizika, kterých si musíte být vědomi před započetím budování jakéhokoliv systému E-Commerce. Také se pokusím osvětlit, jakým způsobem hodnocení a řízení rizik může napomoci v jejich pochopení a kvantifikaci a jak případně vyvážit tato rizika oproti potenciálním ziskům.

3.1.2 Identifikace rizik

Dnešní hrozby pro e-commerce systémy převážně zahrnují:

• **Fyzické hrozby** - hrozby pro IT infrastrukturu, například požár nebo povodeň.

• **Ohrožení dat** - hrozby pro software, soubory, databáze, atd. viry, trojské koně a tak dále..

• **Lidské chyby** - např. otevírání příloh nevyžádaných emailů, ze sociálních sití ale také i nádoné, umyslné či neumyslné smazaní a ztráta dat zaměstnancem

• **Poplašné zprávy** - např. varování o neexistujícím viru či sbírce nebo řetězového emailu, rozesílané e-mailem (tzv. Hoax). Přestože se jedná samo o sobě relativně neškodné formu hrozby, mohou se rychle šířit a způsobit tolik problémů, jako skutečný virus určený k zahlcení e-mailových systémů (DDOS, DOS).

• **Technická selhání** – například chyby v aplikacích, OS, HW

• **Infrastrukturní selhání** - např. havárie serverů, prvků sítě atd.

• **Podvody** s kreditní kartou a jiné platebních podvody.

• **Škodlivé útoky uvnitř nebo vně firmy** - konkurence.

• **Možnost útoku hackera** za různými účely, od získání různách dat, přes jejich poškození až po získání kontroly nad Vaším systémem k jeho dalšímu možnému zneužití ať už k provádění různých DDOS utoků, či použití ditribuovaného výpočetního výkonu k lámání hesel atd. (3, 16, 27)

3.1.3 Typické druhy ohožení v prostředí E-Commerce

• Riziko pro tajné firemní informace a duševní vlastnictví z řed interních zaměstnanců a obchodních partnerů. Je obtížné určit, jak budou citlivé údaje zpracovány třetí stranou nebo smluvními pracovníky. Jen málo organizací má zavedeny systémy pro zajištění společných norem v prověřování zaměstnanců a bezpečnosti mezi obchodními partnery.

• Hackerské využívání chyb v návrhu aplikace, technickém provedení nebo provozních systémech. Kromě toho jsou tato zranitelná místa a techniky průlomu široce zveřejňována a tím vzniká další zvýšená pravděpodobnost hrozby útoků i z řad ne-hackerů a experimetátorů.

• Napadení firemní webová stránky - pokud je firemní stránka nebo její obsah přetvořen či pozměněn, či obsahuje viry, může toto vést ke strátě obchodního jména, reputace, důvěry či firemní image což může vést v konečném důsledku i k přímému dopadu na vlastní podnikání firmy a ztrátě jak obchodních partnerů, tak i místa na trhu.

• Denial-of-Service útoky (DOS, DDOS) - používají záplavu falešných zpráv k havárii nebo zpomalování podnikových systémů - může mít zničující dopad na komunikační a e-commerce aktivity. DOS a DDOS útoky poskytují rostoucí příležitostí pro jednotlivce podniknout takový útok s nízkým rizikem sledovatelnosti. Hackeři stále častěji využívají botnety - skupina počítačů je napadená škodlivým softwarem, který jim umožnuje na dálku v případě potřeby, ovládat tyto systémy a hromadně je využívat právě k takovýmto podobným útokům.

3.1.4 Potenciální dopad při narušení bezpečnosti

Nejsou li po napadení urychleně přijata patřičná opatření, pravděpodoně na sebe nenechají problémy dlouho čekat. Zákazníci E-commerce mají obvykle malou loajalitu, takže pokud vaše webové stránky nejsou k dispozici, není pro ně problém se během několika vteřin přesunout na web jednoho z vašich konkurentů. Kromě toho mohou mít tato technická selhání rovněž významný vliv na vaše obchodní partnery. Je proto důležité, abyste podnikly kroky k zabránění těchto problémům ještě než vůbec započali, neboť je toto mnohem méně nákladné a více efektivní než se snažit reagovat až na vzniklou situaci a na rychlo zalepovat či opravovat škoda a díry v systému. (27)

Současné trendy

Způsob, jakým malware - viry, červy, trojské koně a spyware - jsou použity se také změnily. Infekce je obvykle prvním krokem v procesu zaměřeném na krádeže důvěrných dat nebo otevírání otvorů v zabezpečení pro umožnění přístupu hackerovi k jehío dalšímu využití. Následně je tedy dobré si odpvědět na otázku: „Jak bezpečné je vaše podnikání před viry?“ Pokud odpovíte „ne“ alespoň na některou z následujících otázek, je třeba naléhavě zlepšit ochranu Vašeho podnikání před škodlivám softwarem:

• Máte v počítači nainstalovám systém na obranu před viry?

• Máte-li antivirovou obranu nainstalovánu, skenujete všechny příchozí e-mailové přílohy? Jste si jistí, že pravidelně aktualizujete virové řetězce svého antivirového rogramu?

• Myslíte si, a také vaši zaměstnanci – že víte, jak zjistit pravděpodobné zdroje virů?

• Víte, na koho se obrátit, pokud zjistíte virovou nákazu na některém z vašich systémů? (3, 27)

3.1.5 Ohodnocení rizik

Posouzení rizik vychází z následujících ustanovení:
• pravděpodobnost výskytu rizika
• jeho možný dopad

Posouzení rizik může být buď kvalitativní nebo kvantitativní.

Kvalitativní hodnocení rizika
Znamená stanovit:
• Hrozby,
• kde jsou vaše systémy zranitelné,
• jake prostředky můžete použít k vyhnutí se nebo minimalizaci hrozeb.
Jakmile budou tyto body zjištěny, měli byste být schopni posoudit, zda je riziko vysoké, střední nebo nízká.

Kvantitativní hodnocení rizika
Kvantitativní hodnocení poskytuje hodnotu, může být použita na pokrytí jakékoli ztráty vzniklé v důsledku narušení bezpečnosti. Pravděpodobnost může být použita k měření pravděpodobnost takové události došlo.(16)

Jak vyčíslit rizika
Prostředí E-commerce se opírá o technologie umožnující komunikaci se zákazníkem, jako jsou webové stránky a fóra, stejně jako o další tradiční technologie založené síťovém prostředí. Buďte proto vždy informováni o nejnovějších hrozbách, které mohou napadnout vaše systémy. Tyto nové hrozby mohou a vetšinou jsou zneužity velmi

rychle a každý takový incident může mít velice široký dopad na vaše obchodní aktivity.. Je důležité, aby váš systém řízení bezpečnosti byl pružný a dostatečně reaktivní na řešení těchto nových možných rizik. (27)

Všechna rizika lze kvantifikovat podle jejich pravděpodobnost a možného dopadu na riziko:

1. vysoké
2. střední
3. nízké

Jak probíhá takováto analýza a ohodnocení rizik? Postup je následující:

1. brainstorming veškerých možných rizik za přítomnosti příslušných interních a externích odborníků
2. určitpravděpodobnost výskytu/pravděpodobnost rating (vysoký, střední nebo nízká) pro jednotlivá rizika
3. odhadnout dopad jednotlivých rizik (vysoký, střední nebo nízká)
4. použít matici pro kvantifikaci rizika

Pravděpodobnost	1= nejnižší stupeň ohrožení, 5= nejvyšší stupeň ohrožení		
Vysoká	3	4	5
Střední	2	3	4
Nízká	1	2	3
Dopad	Nizký	Střední	Vysoký

Tabulka 2: Matice kvanifikace rizika

Nejdůležitější rizika jsou označeny stupněm 5, nejméně významná rizika hodnocena jako 1. Jakmile budete mít ohodnocena veškerá možná rizika, můžete určit a odhadnout, kolik času a peněz byste měli obětovat provádění jednotlivých vhodných bezpečtnostních opatření. Například nemá cenu provádět nákladná bezpečnostní opatření u těch rizik, které jsou nepravděpodobné, a které by měly v případě jejich výskytu jen a pouze malý nebo žádný dopad. Na druhou stranu byste měli soustředit

zdroje na vývoj bezpečnostních opatření na rizika s vysoukou pravděpodobností výskystu a vysokým dopadem na vaše obchodní aktivity.

3.1.6 Tvorba bezpečnostního rámce

V běžném životě není nikdy možné naprosto eliminovat všechna potenciální rizika pro vaše podnikání. Toto je způsobeno následujícími faktory:
• neexistuje žádný praktický způsob, jak odstranit hrozbu některých rizik
• odstranění některých rizik je finančně tak náročné, že přijetí opatření na jejich odstranění je značně finančně neekonomické až nerealizovatelné (27)

Proto návrh rámce pro řízení rizik by měl:
• Odrážet, kde spočívají největší potenciální rizika,
• stanovovat konkrétní opatření ke snížení rizik na nejnižší možnou úroveň,
• odrážet náklady a přínosy přijetí opatření k omezení nebo eliminaci rizik.

Použití místních kontrolních skupin je taktéž důležitou součástí každého rámce pro řízení rizik, ale tyto musí být podporovány prostřednictvím politik, standardů a taktéž systémem řízení informační bezpečnosti. (27)

Bezpečnostní politiky
Je důležité mít zavedena pravidla, která upravují a řídí ty činnosti, které by mohly představovat bezpečnostní hrozby. Jedním z nejdůležitějších pravidel je upravení pravidel při využívání přístupu zaměstnanců na internet, politika by měla jasně stanovovat, co je a co není povoleno při využívání firmeního připojení na internet. Další důležitou politikou, která by měla být stanovena je politika využívání firemní emailové pošty, neboť riziko virové nákazy prostřednictvím emailových příloh je velmi vysoké. Jedním z řešení je využití speciálního software pro automatické odebírání emailových příloh z nedůveryhodných, neověřených, či neznámých zdrojů, tak jako odebírání příloh specifického typu (.exe, .bat, .avi atd..) (27)

Standardy

Standardy jsou důležité při vývoji bezpečného prostředí e-commerce. Například, dohodnuté standardy pro zadávání zakázek na PC, servery a firewally vyznamě napomáhají zajistit jednotnost a také významě napomáhají při zvyšování důvěry v technickém prostředí. (27)

Technické kontroly

Tvorba postupů pro pracovníky technické kontroly je další věc zásadního významu, a to zejména tam, kde tito pracovními mají možnost, či dokonce za úkol přiřazovat a odebírat přístupová práva do jednotlivých systémů. Jedním z nejčastějších prohřešku je nezrušení přístupových opravnbění zaměstananům kteří opustili společnost, případně zde pracovali jako dočasně přidělení zaměstnani v rámci kontraktů se subdodavatelskými firmami. (27)

Systém řízení bezpečnosti informací

Plně funkční systém řízení bezpečnosti informací poskytuje rámec, v němž mohou a jsou jednotlivé prvky technické kontroly, politiky, standardy a postupy nadále rozvíjeny, provozovány a přezkoumávány.
ISO / IEC 27001 je mezinárodní norma, která stanoví rámec osvědčených postupů pro informační bezpečnost. (27)

3.1.7 Snižová rizika jeho předcházením a převodem na jiný subjekt

Máte-li na vašich podnikových informačních systémech zjištěna možná rizika, kterým nelze čelit žádným prostředkem technické kontroly, který můžete aplikovat vlastními silami, pak existují další možnosti:

Vyhnutí se riziku

Vyhnutí se riziku je nejvíce efektivní způsob řízení rizik. V zásadě to znamená takové řízení podniku, které už v základu odstraňuje veškeré možnosti vzniku rizika. Například výhýbat se zavádění novým technologií a pod. Na druhou stranu, třebaže tento způsob řízení se může zdát zajisté velice účiným co se vyhýbaní se riziku týče, povětšinou lze

tohoto dosáhnout je velice ztěžka, neboť tlaky okolí (zákazníci, konkurence) na business mohou a povětšinou jsou takové, že s takovýmto způsobe řízením by firma vetšinou směřovala rychlou cestou k záhubě. Snaha vyhnout se riziku nemusí být tedy vždy vhodným řešením pro vaše podnikání, ale stále může tvořit důležitou součást vašeho celkového posouzení rizika. Dokonce i když jste tuto variantu zamítli, budete alespoň dělat rozhodnutí na základě informovaného rozhodování. (16)

Přenos rizika na jiný subjekt

Riziko může být převedeno dvěma způsoby. Prvním z nich je prostřednictvím pojištění. To může být problematické v prostředí e-commerce, jelikož je často velice obtížné vyčíslit ztráty vzniklé v důsledku bezpečnostního incidentu. To je ještě těžší v případě, že škoda byla způsobena v důsledku porušení bezpečnosti ze strany vašeho obchodního partnera.

Druhou možností je uzavřít smlouvu na všechny aspekty vašeho podnikání v rámci e-commerce se třetí stranu. To může zahrnovat například web hosting vašich obchodních aplikací, či provozovaní vašeho obchodního systému na jejich infrastrukuře vaším jménem. An tom je nejvíc důležitá ta vlastnost, že protože je práce s IT technologiem jejich hlavním businessem, operují vetšinou na mnohem bezpečnějších platformách a mají již zavedeny veškeré bezpečnostní standardy a politiky. Nicméně, zatímco v smluvní ujednání lze jasně definovat jaké služby budou poskytovány a za jakých podmínek společně se stanovením případných sankcí za nedodržení smluvních podmínek, primární dopad každého incidentu bude vždy na vaše podnikání. Tato varianta je také obvykle finančně náročnější a je tedy dobré opravdu zvážit, zdali tuto možnost a do jaké šíře služeb využít. (16)

Snižování pravděpodobnosti rizika

Protože nikdy zcela nemůžete eliminovat rizika ohrožující vaše podnikání, je proto třeba naplánovat, jak budete tato rizika v maximální míře eliminovat. Jedná se defacto o 2 skupiny činností.

a) Redukce možných hrozeb

Redukovat hrozby pro systémy E-commerce systému je možné následujícími způsoby:

• Udělat z podnikání menší cíl – zvážit, co je opravdu pořeba zveřejňovat na veřejných nebo sdílených systémech a tam, kde je to možné, odstranĕit veškeré citlivé obchodních informace,

• zvýšit veřejné vnímání firmy jako maximálně zabezpečné - zajistit, aby všechny potřebné aspekty bezpečnosti byly dobře a viditelně nainstalovány a řízeny,
• zajistit, aby varování pro uživatele vstupující do zabezpečené zóny vaší internetové stranky, byly jasně viditelné,

• neuvádĕt veřejně podrobnosti o používaných způsobech zabezpečení jakýchkoliv vámi používaných systémů, jakožto ani informace o vámi používaných platformách,

• pravidelně aktualizovat používanýé antivirové programy a být neustále informován o všech nových možných hrozbách k přijetí patřičných opatření,

• zajistit proškolení všech zaměstnanců, jak správně zacházet s firemním emailem a připojením k internetu, že např. nemají otevírat přílohy z neznámých zdrojů, klikat na podezřelé odkazy či přeposílat zprávy typu „zaručených zpráv“ s žádostí o rozeslání co nejvíce lidem, různé řetězové emaily a pod.,

• konfigurace e-mailových systémů k otevírání příloh pomocí „vieweru“, aby se zabránilo možné infekci makro viry ukrytými uvnitř souborů.

b) Redukce možnosti průniku

Medoty na snižování možnosti průniku do systémů E-commerce jsou založeny na znalostech jejich slabých míst a přijetí následných opatření zaměřených na snížení nebo odstranění těchto slabin. Mezi typická opatření patří:

• Instalace brány firewall pro filtrování siťového provozu a zabránění nelegitimních pokusů o přístup do systému. Tyto systémy by měly být správně nakonfigurovány a měla by mít implementována pravidla, která odrážejí potřeby firmy.

• Implmentovaný „silný“ autentizační proces. Toto má za účel zaručit jednoznačnou identitu uživatele a zaručuje také mnohem vyšší bezpečnost než systémy používající

k přístupu pouze heslo. Poslední dobou se zvyšuje počet dostupných řešení založených na bázi tzv.“Smart-Cards“ nebo biometrických systémech. Hlavní myšlenka byse však měla upírat směrem k 2.stupňové autorizaci, která je založena na myšlence, že za 1. něco vlastním, a za 2. něco znám. Třeba kombinaci přístupové Smart karty a osobního přístupového kódu.

• Využití digitálních certifikátů k zajištěnít důvěry mezi jednotlivci, systémy a obchodními partnery. Tyto poskytují bezpečnou komunikaci za pomoci ověřování identit jednotlivců, systémů nebo organizací za pomoci digitálního popisu a tímto chrání jednotlivé transakce před možným zneužitím a jasně identifikuje komunikující strany.

• Zavedení virtuálních privátních sítí (VPN), k poskytnutí zabezpečeného komunikačního kanálu pro své obchodní partnery k bezpečné výměně informací při využití internetu.

• Instalace všech dostupných bezpečnostních patchů pro operační a zabezpečovací systémy, k zajištění minimalizace možného průniku do vašeho systému z venčí za pomoci využití známých slabých míst.

3.1.8 Deset bodů efektivního řízení rizik

V následujících 10-ti bodech se pokusím nastínit jak rozvinout a realizovat efektivní strategii pro řízení rikik v prostředí E-Commerce. Tento 10-ti bodový plán je založen na využití normy ISO / IEC 27001:

• Setřídit rizika do skupin v kontextu E-commerce, identifikovat změny oproti tradičním rizikům IT systémů a zjistit nové potenciální hrozby specifické pro prostředí E-commerce.

• Vzít v úvahu možnosti, schopnosti a motivaci potenciálních útočníků.

• Provádět pravidelná hodnocení rizik. Vytvořit účinný systém řízení a dokumentace incidentů, který zahrnuje všechny prvky prostředí E-commerce.

• Vytvořte váš systém E-commerce v efektivním rámci informační bezpečnosti.

• Zvažte certifikaci podle ISO / IEC 27001 pro vaši firmu a vaše obchodní partnery.

• Implementujte standardní konfigurace pro počítače, servery, firewally a jiné technické prvky systému.

• Nespoléhejte se pouze na jediný systém kontroly. Většina bezpečnostních odborníků doporučuje nejméně „dva faktory“ ověřování identity uživatele, jako například něco, co jste (např. občanský průkaz) a něco víte (PIN/heslo).

• Podpořte všechny stupně kontroly patřičnými policies, procedůrami a zvyšování povědomí o nich.

• Vytvořit integrované plány kontinuity podnikání pro všechny kritické E-commerce aplikace.

• Provádějte pravidelné kontorly a analýzy rizik pro zjištění účinnosti implementovaných řešení.
(27)

3.1.9 Norma ISO/IEC 27001

Norma ISO/IEC 27001, která je součástí rodiny norem ISO/IEC 27000, je norma pro ISMS (Information Security Management system), která byla vydána v říjnu 2005 organizací ISO a IEC. Firma která přijme standart za svůj, může být pro tuto normu po splnění patřičných požadavků certifikována opravněnou společností. Certifikace probíhá jako u ostatních ISO certifikací 3 fázově. (22)

Charakteristika normy

Norma řeší osvědčeným způsobem bezpečnost informací s cílem řídit rizika s touto problematikou související, ať už se jedná o technologie nebo prostory. Cílem je poskytnout doporučení, jak správně aplikovat ISO/EIC 17999 (v budoucnu 27002). Z tohoto důvodu jsou hlavní části ISO/EIC 27002:2008 uvedeny v příloze ISO/IEC 27001. Interpretace a implementace se může lišit v návaznosti na rozsahu systému, druhu a způsobu zpracování dat, jejich hodnotě, atd. Pokud je systém řízení bezpečnosti informací zaveden pouze v určité části organizace, vydaný certifikát je platný právě pro tuto část nikoli pro celou organizaci. Norma prosazuje procesní přístup a je plně kompatibilní s ostatními systémy (ISO 9001, ISO 14001, atd.), lze ji proto certifikovat nejen samostatně, ale i integrovaně. (22)

Komu je norma ISO 27001 určena

Všechny organizace, které si chtějí uspořádat své informace podle důležitosti a mají v úmyslu k nim přistupovat systematicky, najdou v této normě praktického průvodce. Systém managementu dle požadavků normy ISO 27001 je určen všem organizacím, které chtějí získat nejen konkurenční výhodu, ale které chtějí chránit svá informační aktiva s vysokou hodnotou a tím minimalizovat ztráty způsobené jejich únikem. Ti, kdo nakládají s citlivými informacemi nebo osobními údaji mohou touto cestou předejít

finančním postihům a trestům, vyplývajících ze zákona, při úniku informací nebo neoprávněným nakládáním s osobními údaji. (22)

Přínosy zavedeného systému

- Zlepšení image organizace, vyšší důvěryhodnost pro zákazníka.
- Celkové posílení stávajícího systému managementu organizace.
- Uvědomění si slabých míst organizace z hlediska bezpečnosti informací, optimální rozložení nákladů na zvýšení bezpečnosti informací a jejich minimalizace (většina účinných opatření zpravidla nevyžaduje velké investice)

Zavedený systém:

- Zajistí včasnou dostupnost informací,
- zamezí nechtěné modifikaci informací,
- zabrání zneužití informací,
- vyloučí možnost ztráty informací.

3.2. Incident management

3.2.1 Úvod

Když systémy nebo procesy selžou, velice rychle se může něco vážného stát. Části světové ekonomiky se mohou zastavit, obchodní procesy mohou zkolabovat, tak jako se můžou zastavit důležité komunikační toky. Když tyto incidenty nastanou, IT organizace musí být připravena řídit každý z ních až k jejich úplnému úspěšnému vyřešení. Může se tedy nakonec stát, že to, jak dobře IT organizace spravuje své incidenty, bude v konečném měřítku považováno za základní metriku pro hodnocení celkového výkonu jeho IT. Efektivní Incident management program umožňuje organizaci účinně sharňovat záznamy o mimořádných událostech, stanovovat priority incidentů a řídit jejich řešení. Proaktivní Incident management program kombinuje služby, technologie, procesy, a informace k minimalizaci dopadu incidentů v oblasti IT na organizaci. Proto se budu v této kapitole věnované Incident managementu sanžit o

nastínění několik osvědčených postupů, které pomáhají organizacím stát se více efektivní a proaktivní při zvládání krizí. (9, 18, 22)

3.2.2 Význam řízení incidentů

Incidenty se stávají v systémech IT každý den, a výzvou zde, kromě stresu a obav z jejich dopadu, které způsobují, je zabývat se jejich účinným zvládáním. Zatímco implementace slabého, neefektivního Incident managementu může mít negativní dopady na podnikání, může implmentace výkonného Incident managementu skutečně uspořit organizaci spoutu výdajů a zdrojů možných upotřebit někde jinde. Co by se například stalo, byla-li by databáze účetního systému společnosti poškozena a znemožnilo by to tudíž zaznamenávání veškerých účetních případů a vystavovavní faktur zakazníkům? Nedostatečná reakce na takovýto incident by mohla znamenat ztrátu v řádech milionů vašich příjmů, což následně může vést až k ohrožení celkové životaschopnosti firmy. Zatímco přínosy dobře organizovaného procesu krizového řízení jsou zřejmé ve výše popsané situaci, existuje mnoho dalších oblastí, kde tyto přínosy již tak zřejmé nejsou, přesto jsou stále pro vaší společnost důležité. Jedníz z takových „obyčejných“ incidentů by mohl být například nemožnost přístupu řadového pracovníka do systému, kterýá je klíčová pro vykonávaní jeho práce. Pokud se vyřešení problému pohybuje v rámci hodin (vetší část jeho pracovní doby), společnost ztrácí produktivitu. Taková ztráta pro jednu osobu se nemusí zdát jako mnoho, ale pokud se tyto ztráty produktivity násobí na tisíce případů ročně, dopad na společnost může být a je ohromující. To je důvod, proč dobře řízený Incident management program může poskytnout cenné úspory na zdrojích organizace. Toto také podporuje tvrzení a konstatování úspešných IT manažerů, kteří poukázují na krizové řízení jako na jeden z nejdůležitějších prvek systému ITIL, procesního modelu pro dodávku a řízení IT služeb. (9, 18, 22)

3.2.3 Incident management

Všeobecně jako definice Incidentu se uvání, že Incident je jakákoliv událost, která není součástí běžného provozu organizace a způsobuje, nebo může způsobit přerušení poskytování služeb IT. V této souvislosti je Incident management proces zajišťující obnovení normální provozu IT tak rychle, jak je to možné a zároveň minimalizuje dopad v rámci definované úrovni služeb. Je důležité si uvědomit, že Incident management je o obnovení původního stavu a nezabývá se otázkou řešenjeho příčiny. Takže Incident management má za hlavní úkol reagovat na vzniklé incidenty, avšak díky sdílení informací, jejich integrací do systémů na dokmentaci incidentů a následnému jejich uspořádání se stává i proaktivní částí k předcházení incidentů, přičemž úzce spolupracuje s ostatními oblastmi IT. ITIL a Mezinárodní organizace pro normalizaci (ISO) definovalo pět klíčových oblastí „best practices“ (osvědčených postupů) pro správu incidentů:

• Detekce a záznam,
• klasifikace, stanovení priorit a sledováník
• zkoumání incidentu, eskalace, a diagnóza,
• řešení a obnova,
• uzavření a komunikace. (23)

Zatímco každá organizace si Incident management program upravuje dle jeho vlastních požadavků, je důležité při jejich tvorbě dodržet tyto osvědčené postupy spolu s výběrem vhodných služeb a technologií na podporu své činnosti.

3.2.4 Výzvy spojené s Incident managementem

Při prvním pohledu se implementace prvků Incident managementu může zdát snadná a triviální. Bohužel, některé úpravy, programy, projekty a aktivity ve jménu efektivity mohou opravdu reálně zkomplikovat jeho implementaci. Největšími viníky tohoto jsou v dnešním Incident managementu jsou:

• Otevřené sítě - organizace spolupracuje se zákazníky a dodavateli, IT systémy a sítě se propojují – vytváří se více bodů možných poruchy a vnější závislosti na konfiguraci.

• Heterogenní systémy - organizace nákupují a používájí různé druhy serverů, operačních systém a zálohovacích zařízení. V těchto heterogenních prostředích vzniká více příležitostí pro incidenty díky interoperabilitě a různorodé konfiguraci.

• Servisně-orientované architektury (SOA) - základy, na nichž je postavena SOA tvoří široká škála služeb, které musí spolupracovat pro jejich řádnou funkci. Incident, jež vznikne na jedné klíčové součást SOA může vytvořit zmatek v celeém řetězci a tak velice ztížit jeho řešení.

• Změna zdroje incidentů - během posledních deseti let, se hardware systémy staly výrazně spolehlivější a zároveň stále více se integrují. V důsledku těchto obou trendů, jsou systémy náchylnější spíše k "měkkým" selháním, jako jsou chyby a konflikty konfigurace, které jsou mnohem obtížnější na diagnostiku a řešení než jednoduše identifikovatelná hardwarová závada. Tato nová éra úkolů vyžaduje, aby IT organizace věnovaly zvláštní pozornost návrhům a nasazení svých Incident mamagent programů. Tyto programy musí reflektovat a přizpůsobovat se novému prostředí IT, jež se stává stále sofistikovanějším a propracovanějším. (9)

3.2.5 Základy řízení incidentů

Vzhledem k tomu, že organizací zabývající se standardy, jako je ITIL, ISO, a COBIT4 popisůjí zeširoka veškeré nejlepší postupy pro správu incidentů, nebudu se zde zabývat

všmi těmito prvky detailně.
Spíše se budu snažit poukázat na některé racionální kroky, které můžeme podniknout ke zlepšení výkonu Incidentnt managementu ve své organizaci na základě právě těchto „best practices“.

• Reakce na událost – v tom nejjednodušším smyslu, Incident management je o reakci na sudálostí reportované uživately IT služeb, když něco nejde tak, jak má. Chcete-li zachovat pořádek a mít jistotu, že IT department je schopen reagovat na všechny objevivší se incidenty, je nutné implementovat některé základní procesy. Společný service desk by měl být ústředním bodem pro příjem, záznam, eskalaci a správu všech incidentů na základě společného postupu. Přestože společný service desk a definované procesy jsou velmi základní krok, slouží jako důležitý základ pro cestu organizace ke správné funkci Incident managementu. (23)

• Nastolit řád v SLA (Service Level Agreement – dohoda o úrovni služeb) - poté, co jednou začnete systematicky evidovat incidenty, budete muset stanovit způsob, jak je třídit a prioritizovat. Prioritizační a klasifikační schéma na základě pořadavků na dodávku servisu je tou nejlepší možností. Pokud má organizace formalní SLA mezi IT a obchodními jednotkami, toto se může jednoduše stát výchozím bodem pro stanovení a klasifikování priorit. Pokud ne, je toto nutné stanovit vse spolupráci se všemi zainteresovanými stranami na základě jjejich pořadavků, případně tyto poznatky sesbírat na jednáních s vašimi obchodními partnery. Toto ujednání poslouží zejména pro předcházení různým konfliktům mezi dodavatelem a odběratelem služby a navíc zajišťuje, že služby jsou doručovaný v souladu se strategií a požadavky organizace. (23)

• Používání norem – o něco výše jsem odkazoval na různé rámce a standardy, jako jsou ITIL, ISO, a COBIT. Všechny tyto řidící rámce věnují zvláštní pozornost krizovému řízení a definují řadu osvědčených postupů. Přijetí těchto norem je volba zavisející na každé organizaci zvlášť, ale jejich základní principy může využít kdokoli. Použití těchto standardů v praxi a znalost jejich „best practices“ je velmi doporučovaná. Tyto osvědčené postupy vám mohou pomoci zlepšit vaše postupy a připravit organizaci pro jejich realizaci, v případě, že se rozhodnete implpmentovat některý z nich. (23)

3.2.6 Proaktivní Incident management

Zatímco se práce incident manažera může zdát nevděčná, je zde určitá naděje na její zhodnocení. Incident management program může být velmi proaktivní ve svém přístupu a může hrát klíčovou roli při minimalizaci celkových dopadů incidentů v oblasti IT na provoz společnosti. V následujících bodech jsou některé velmi jednoduché, ale zároveň velmi účinné kroky jak se stát proaktivním v rámci Incident managementu. (18)

• Sdílení informací – přístup k informacím je pro Incident management jedním z nejdůležitějších bodů k zvýšení jeho schopnosti řešit případy rychle a efektivně. Informační zdroje, jako change management systém, nebo „knowledge base“ (database znalostí), hrají klíčovou roli. Tyto systémy nabízejí identifikaci známých problémů, doporučené postupy řešení a náhradní řešení, a upozorní vás na potenciální problémy. Použití těchto prostředků je proaktivní krok, který můžete při řízení incidentů využívat a je to jeden z ITIL „best practices“. (18)

• Integrace s ostatními IT procesy - úzké propojení Incident managementu s Problem a Configuration managementem zlepší výrazně schopnost sdílet informace a spravovat incidenty proaktivně. Problém management proces zajišťuje v organizace odhalovaní a nápravu příčin problémů. Úzké vazby na Configuration management poté umožňuje odhalení potenciálních problémů vzhledem ke konfiguracím systémů a možnost jejich vyřešení ještě před samotným jejich vznikem. (18)

• Automatizace – každá IT organizace by měla usilovat o automatizaci procesů, kdykoli je to alespoň trochu možné, a Incident management proces není žádnou výjimkou. Automatizace je důležitá, protože minimalizuje chyby způsobené lidským faktorem při zpracování, usnadňuje rychlejší doby odezvy a pomáhá zajistit dodržování procesu. Existuje bezpočet možností pro automatizaci procesů související se správou incidentů, od software určeným pro help-desky ke sledování životního cyklu incidentu až po automatizované monitorování a automatický alerting v případě poruchy monitorovaných systémů. Co je důležité, je výběr a posléze použití automatizace. Zvolit vhodnou strategii a nakoupit a používat pouze takové automatizační nástroje, které mají

smysl pro vaši organizaci, které vám pomohou spravovat vaše incidenty účinněji a efektivněji. (18)

3.2.7 Tři jednoduchá pravidla Incident managementu

Pravidlo 1 - Incident management je kritický pro efektivní řešení veškerých incidentů, které mají jakýkoliv dopad na vaše podnikání. I malé incidenty se mohou po sečtení vyšplhat k takovým nákladům, že mohou dokonce ohrozit vaše podnikání.

Pravidlo 2 - Incident management je správa informací - Incident management je především o informacích – informacích o incidentu a o tom, jak službu co nejrychleji obnovit. Zdroje informací , jako jsou Change management, Configuration management či znalostní databáze mohou být nejlepším zdrojem informací pro efektivní řízení incidentů.

Pravidlo 3 – Incident management může být proaktivní. Zatímco Incident management se může zdát jako systém, který reaguje až na vzniklé problémy, i přesto to může být proaktivní. Procesy jako automatizace, integrace a sdílení informací jsou osvědčené postupy, jak udělat Incident managemnt také významnou poraktivní složkou při zvládání krizí.

3.2.8 Shrnutí

Zatímco se Incident management může zdát být nevděčná práce, je to základní proces, které každý IT oddělení musí zvládnout. Incident management je pilířem, který spojuje komunitu uživatelů IT služeb s prostředky pro řešení mimořádných událostí v rámci IT prostředí. Incident management identifikuje, klasifikuje, a řídí řešení incidentů a zároveň minimalizuje jejich dopad na podnikání. Tato role je rozhodující pro zajištění toho, že dopad incidentů v oblasti IT na vlastní podnikání je řízen efektivně. A nabízí nadějí, že dopad budoucích události může být zmírněn či případně se mu dá zcela předejít, tak jak se Incident management bude stávat stále proaktivnějším.

4. Návrh vlastního řešení a jeho přínosy

4.1 Implmenetace Incident managementu do organizace zabývající se E-Commercí

V této praktické části mé diplomové práce se pokusím navrhnout model Incident management desku pro suport organizace zabývající se (nejen) E-Commercí. Tato část bude vytvořena formou projektu. Model incident desku by měl zaručovat plně hodnotný servis v 12h směnném modelu s pokrytím 24/7/365 a samozřejmě by měl poskytnout umožnění naplnění cílů, které budou v projektu stanoveny. Součastí projektu bude jak analýza rizik projektu tak kompletní WBS (work breakdown structure) s vyhledáním critické cesty za pomoci CPM. Na závěr vyhodnotím přínosy projektu a uzavřu práci pohledem na celkovou problematiku v současném světě.

4.2 Logický rámec projektu IM

IM	**Popis projektu**	**Objektivně ověřitelné Ukazatele**	**Způsob ověření**	**Předpoklady / rizika**
Vyšší cíl	Maximalizace availability zákaznického objednávkového systému a minimalizace nákladů na udržení servisu na požadované výší	Availabilita systému pro zákazníka, náklady na služby IM	1. Měsíční kontrola plnění stanovených SLA, měsíční kontrola nákladů	1 Podaří se zajistit kvalitní servisní organizaci
Cíle	1. Vytvoření IM, MOD a ProbMan. 2. Zachování zaměření organizace na její hlavní business 3. Zprůhlednění a zefektivnění interní komunikace a odpovědnosti.	1.IM, Prob.Mn a MOD k dispozici, pravidelný reporting dle dohodnutých termínů 2. Veškeré služby ohledně zavedení projektu IM outsourcingované 3. Komunikační matrice jako součást základních podnikových procesů	1.Kontrola plnění dohodnutých SLA 2 Kontrola organizačni struktury společnosti 3. Prověrka obsahu podnikových procesů .	1 Naplnění požadavků společnosti servisní organizací. 2+3 Důkladnáé plánování a kontrola
Výstupy	1. IM team pro komunikaci s organizací 2. Vytvořeni a distribuce komunikační matrice	1. Team lidi zodpovědných za komunikaci s outsourcingovou organizací. 2. Komunikační matrice zkontrolována a schválena vedením.	1. Kontrola R&R v matici organizece 2. Kontrola zápisu ze schvalovacího jednání	1 až 2 Projekt bude probíhat podle plánu
Klíčové činnosti	1. Vytvoření IM teamu 2. Tvorba komunikační matrice	1. Navržení kandidátů. 2. Vytvoření kom.unikační matrice	1. Prověrka přihlášek 2. Prověrka záznamů připomínkového řízení	1. Dostatečný zájem pracovníků 2 Dobré zmapování organizační struktury

Tabulka 3: Logický rámec projektu

4.3 Identifikační listina projektu

Název projektu: Transformace Incident managementu (projekt IM)
Identifikační číslo projektu: IP 06/2011

Charakteristika projektu: Projekt řeší transformaci Incident managementu do praxe firmy v rámci projektu minimalizace dopadů technických problémů na chod zákaznického systému.

Zahájení projektu: Datem vyhlášení projektu
Ukončení projektu: do 30. 06. 2012

Plánované náklady na projekt: 1 553 064 Kč

Cílová odměna: 30 000 Kč (bude vyplacena na základě úspěšných kontrolách v měsíci březnu 2003)

Projektový tým:

Vedoucí projektového teamu	1
Ekonomický poradce	2
SM specialista	2
IT poradce	2
HR specialista	1
Finanční manager	1

Schválený návrh projektu	
Kontrola výsledů výb.řízení	
Podpis smlouvy s vybranou firmou	
Kontrolní den s vedením firmy	
Začátek transition fáze	
Kontrola implementace IM	
Kontrolní den s vedením firmy	
Začátek pilotního testovaní	
Kontrola vysledků pilotu	
Přechod na ostrý provoz	
Ukončení projektu	

Tabulka 4: Tabulka milníků projektu

Specifikace cílů projektu: viz příloha č.1 Logický rámec projektu

Rekapitulace přímých nákladů projektu IM

Náklady na výběrové řízení	20 000 Kč
Mzdové náklady pro členy project teamu	1 000 000 Kč
Školení pro IM team	200 000 Kč
Kurz ITIL	64 000 Kč

Cílová odměna	270 000 Kč
Posouzení návrhu projektu	5 000 Kč
Oponentura komunikační matrice	8 000 Kč
Rezerva	50 000 Kč
Celkem	1 553 064 Kč

4.4 Analýza kritických faktorů úspěchu

Jako kritický faktor úspěchu byl označen fakt:

- snížení a omezení výpadků obchodní aplikace na minimum, a tím zajištění dramatického nárůstu spolehlivosti a výkonnosti, což zajistí posílení důvěry a věrnosti zákazníků.
- zvýšení spokojenosti zákazníků s nabízenými službami s odrazem na ekonomické výsledky společnosti.
- zlepšení vnitrofiremní komunikace v případě vyskytnutí se výpadku na infrastruktuře a tím ke zkrácení těchto výpadků na nejnižší možnou dobu – maximalizace availability
- navázaní dobrých vzájemných vztahů s outsourcingovou organizací na bázi profesionality a vzájemného pochopení potřeb a tím zajištění požadovaného servisu na požadované urovni.

4.5 Cíle projektu

4.5.1 Incident management a jeho úloha

Cíle a hlavní aktivity Incident managementu:

- Obnovit normální provoz služby, a to co nejrychleji při současné minimalizaci důsledků výpadku služby na provoz (tzn. na zákazníky a uživatele)
- Zajišťovat, aby služby dodávané zákazníkům splňovaly kvalitu podle dohodnutých Service Level Agreements

Incident management je odpovědný za včasnou detekci incidentů, jejich zaznamenávání a řízení jejich životního cyklu. Jeho cílem je "být co nejrychlejší", Incident management v zásadě vůbec nezkoumá PROČ k incidentům dochází, ale hledá jakékoli řešení vedoucí k obnovení služby (za hledání příčin incidentů je odpovědný Problem Management)

Přínosy implementace Incident managementu:

Pro obchodní podnikání organizace:

- Snížení důsledků dopadu incidentu
- Proaktivní identifikace možností zlepšení
- Dostupnost manažerských informací vztahujících se na Service Level Agreements

Pro úsek informačních technologií:

- Přesné měření míry plnění Service Level Agreements
- Manažerské informace o aspektech kvality služeb
- Lepší využití zdrojů, efektivita práce
- Eliminace "ztracených incidentů"
- Věrohodnější obsah CMDB
- Zvýšení spokojenosti zákazníků a uživatelů

Důsledky neexistence procesu Incident managementu:

- Neřízené incidenty se "ztrácejí", při špatně řízených incidentech se prodlužuje doba jejich odstranění, a tím se prodlužuje i doba výpadku služby.
- Neexistence eskalačních procedur způsobuje, že se z drobných incidentů stávají incidenty závažné, které významně ovlivňují kvalitu služeb
- Specialisté v skupinách podpory jsou neustále vyrušováni ze své práce, a tím se dostávají do časového presu
- Řešení incidentů přístupem "já si myslím ..." namísto "já vím ..."
- Vyrušování pracovníků obchodu, na nichž se obracejí jejich kolegové s žádostí o radu

- Nedostatek koordinovaných manažerských informací

4.5.2 Definice konkrétních cílů projektu

- Postupné nahrazení služby Manager on Duty
- Vedení denních status callů pro určeného zákazníka a správa a údržba dat na servis management internet portálu
- Řízení a vedení řešení všech incidentů s vysokou prioritou (klass. Severity1 a Major incident), působí jako counterpart pro SDM/DPE/AITA and DSL + IT specialisty přes všechny spravované zákazníky
- Otvírá, aktualizuje a zavírá globální informační alertovací databázi a spravuje a aktualizuje internetový Alert board.
- Office time pro Incident desk je 24/7/365 (nepřetržitý provoz) ve 12h směnách
- Umístění teamu Incident desku by mělo být co nejblíže umístění ostatních teamů pracujících pro stejného zákazníka z důvodu vetší průžnosti při řešení problémů.
- Zajištění maximální customer satisfaction v rámci kontraktovaných SLA

1. Nahrazení služeb MOD (Manager on Duty servisu)

- Soustředit služby poskytované MOD do jednoho bodu namísto zřizování customer specific MoD pro každého zákazníka zvlášť
- Po nastartovaní produkce přebrat zodpovědnost za MoD a vykonávat činnost v jejich zastoupení s polu s kompletní MOD agendou.
- Tvorba měsíčních MoD reportů
- Analýza MoD reportů a na jejím základě navrhovat řešení k zvýšení porduktivity

2. Vedení denních service status callů

- Příprava Denní služba Stav volání a mít k dispozici informace připraveno 8 hodin ráno
- zahájení a vedení hovoru, prezentovat získané informace a reagovat na ad hoc informatipon poskytované během hovoru

- Vedle zpráv o stavu informační Incident (pro Incidenty Priorita 1 jediný), a problém nahrávat aktualizace
- Repond na inquieries, kde nebyly dostupné žádné údaje během přípravné fáze
- Sledování návaznosti na otevřené položky z předchozích výzev
- Incident recepci nebude repsonsilble řídit Změnit poradní výbor (MCAB), podávání zpráv o provozních záležitostech a Cross Compliance otázky ITDelivery jako součást výzvy Stav služby

3. Správa všech Prio 1 a major incidentů:

- Řízení mimořádných událostí a krizových situací a působnost jako hlavní kontakt pro servis delivery manažery, DPE , IT specialisty, IT architekty, technickal solution manažery a / nebo zákazníka.
- Zahájení major incident procesu po konzultaci s DPE
- Na požádání: Poskytování informací top managementu v čase trvání incidentu.
- Produkovat Management informací o všech mimořádných událostí Pri 1 a major, ke kterým došlo v průběhu posledních 24 hodin.
- Pro vikendy a bank holiday: vykazované období se prodlouží na 48 nebo 72h
- Sledovat akční plány (tj. činnosti v záznamech Problem managementu), sledování dostupnosti RCA a spravuje RCA kvality

4. Otevírání (iniciace), aktualizace a uzavírání globálních informačních alertů (AMI) a udržování Alertboardu na intranetu (Wiki):

- Otevírat a aktualizovat AMI záznamy včas, spolu s uvedením všech požadovaných informací (pouze pro zákazníky, dohodnuté v kontraktu)
- Trackovat AMI alerty až do finálního vyřešení incidentu, provádět follow-up aktivity na dosud nevyřešené incidenty a reporty MoD (manager on duty)
- Aktualizace AlertBoardu na intranetových stranách SM (service management)

4.6 R&R (Roles and responsibilities)

Incident Desk Managerovi je dána pravomoc řídit incidenty efektivně přes první, druhý a třetí level podpory

- Řízení činnosti teamů podílejících se na řešení incidentů, spolupráce s vedoucími produkčních teamů
- Monitorování účinnosti Incident managementu a řízení a navrhování zlepšení z hlediska účinnosti a efektivity
- Schopnost přijímat rozhodnutí ovlivňující produkci a podílet se na řešení závažných incidentů i nad rámec pracovní doby

Osobní předpoklady pro osobu Incident managera:

- Má minimálně 2 roky praxe se service delivery v mezinárodním prostředí, praxe s vedením lidí s vůdčímy schopnostmi, dobré znalosti v klíčových procesech Incident a Availability Managementu.
- Znalost E2E service delivery modelu spolu s technickým backgroundem (nejlépe IT), schopnost samostané práce a rozhodování se, schopnost sebemotivace, velmi dobré vyjednávací a komunikační schopnosti, stejně jako dobré prezentační dovednosti
- Silný týmový hráč, spolehlivý, vysoká odolnost proti stresu

Stanovení počtu pracovníků na pokrytí uvažovaného Incident desku

- Plánovaná pracovní doba Incident desku je 7/24/365
- Jsou plánovány 12h pracovní směny v časových intervalech 06am-18pm, 18pm–06a.m
- Pokrytí směn je plánován na 2FTE/day a 1FTE/night (minimální pokrytí alespoň 1FTE/shift)
- Koeficient pro pokrytí absencí je 0.8

S přihlédnutím k zákonným přestávakám dle českého práva je minimální počet FTE k udržení servisu bez přihlédnutí k absencím 6FTE. Po vynásobení koeficientem 0.8 dostáváme 7,5FTE. Po přihédnutí k minimálnímu počtu obsazení směn alespoň 1 osobou na každou směnu, je v konečném důsledku v této fázi hledám počet 7 FTE celkem.

4.7 Mapa rizik navrženého projektu

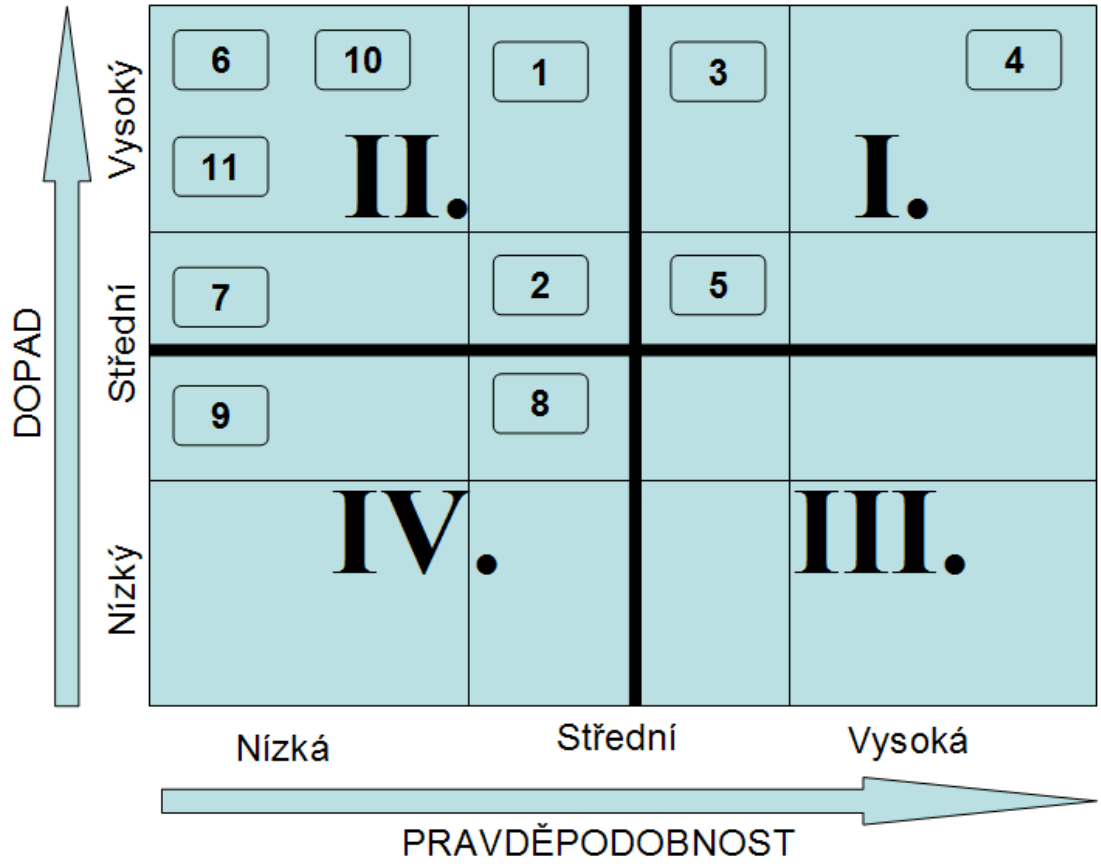
Mapa rizik nám umožňuje graficky znázornit rizika spojená s projektem a zaměřit se převážně na tzv. klíčová rizika, která se nacházejí v růžové oblasti „Vysoké riziko“ na následujícím obrázku. Dále hodnotíme rizika na hlavní (žlutý segment) a běžná (zelený segment).

Při tvorbě mapy rizik k mému modelovému projektu jsem postupoval ve 2. krocích:

- tvorba tabulky rizik s ohodnocením jejich dopadů a pravděpodobnosti výskytu
- zanesení těchto rizik dle údajů z tabulky od grafické podoby

č.r.	Mapa rizik - data sheet Riziko	Dopad	Pravděpodobnost výskytu
1	nedostatek vhodných kandidátů	vysoký	střední
2	neochota předání znalostí	střední	střední
3	legislativní překážky	vysoký	střední
4	zásah odborů	vysoký	vysoká
5	špatný odhad rozsahu práce	střední	střední
6	nepotřebnost pozice	vysoký	malá
7	zdravotní problémy	střední	malá
8	nedodržení timeline	střední	střední
9	překročení budgetu	střední	malá
10	zrušení projektu	vysoký	malá
11	špatně nastavené požadavky na kandidáty	vysoký	malá

Tabulka 5: Tabulka rizik projektu



Obrázek 8: Umístění rizik projektu do mapy rizik

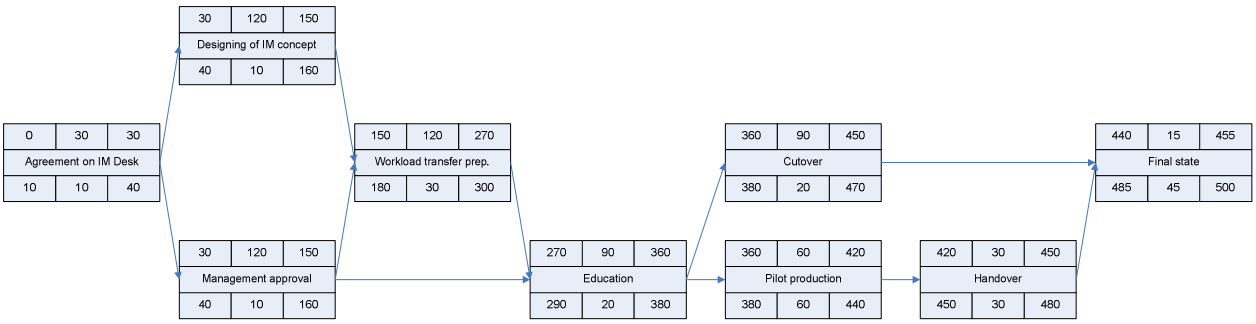
4.8 Časový plán projektu

i	Jméno činnosti	čas trvání (dny)	předchůdce (i)	ZM	KM	ZP	KP	R
1	Agreement on IM Desk	30		0	30	10	40	10
2	Designing of IM concept	120	1	30	150	40	160	10
3	Management approval	120	1	30	150	40	160	10
4	Workload transfer prep.	120	2,3	150	270	180	300	30
5	Education	90	3,4	270	360	290	380	20
6	Pilot production	60	5	360	420	380	440	60
7	Handover	30	6	420	450	450	480	30
8	Cutover	90	5	360	450	380	470	20
9	Final state	15	7, 8	450	465	485	500	45

Tabulka 6: Časový plán projektu

Legenda:

ZM	Doba trvaní	KM
Jméno činnosti		
ZP	Rezerva	KP



Obrázek 9: Analýza projetku metodou CPM

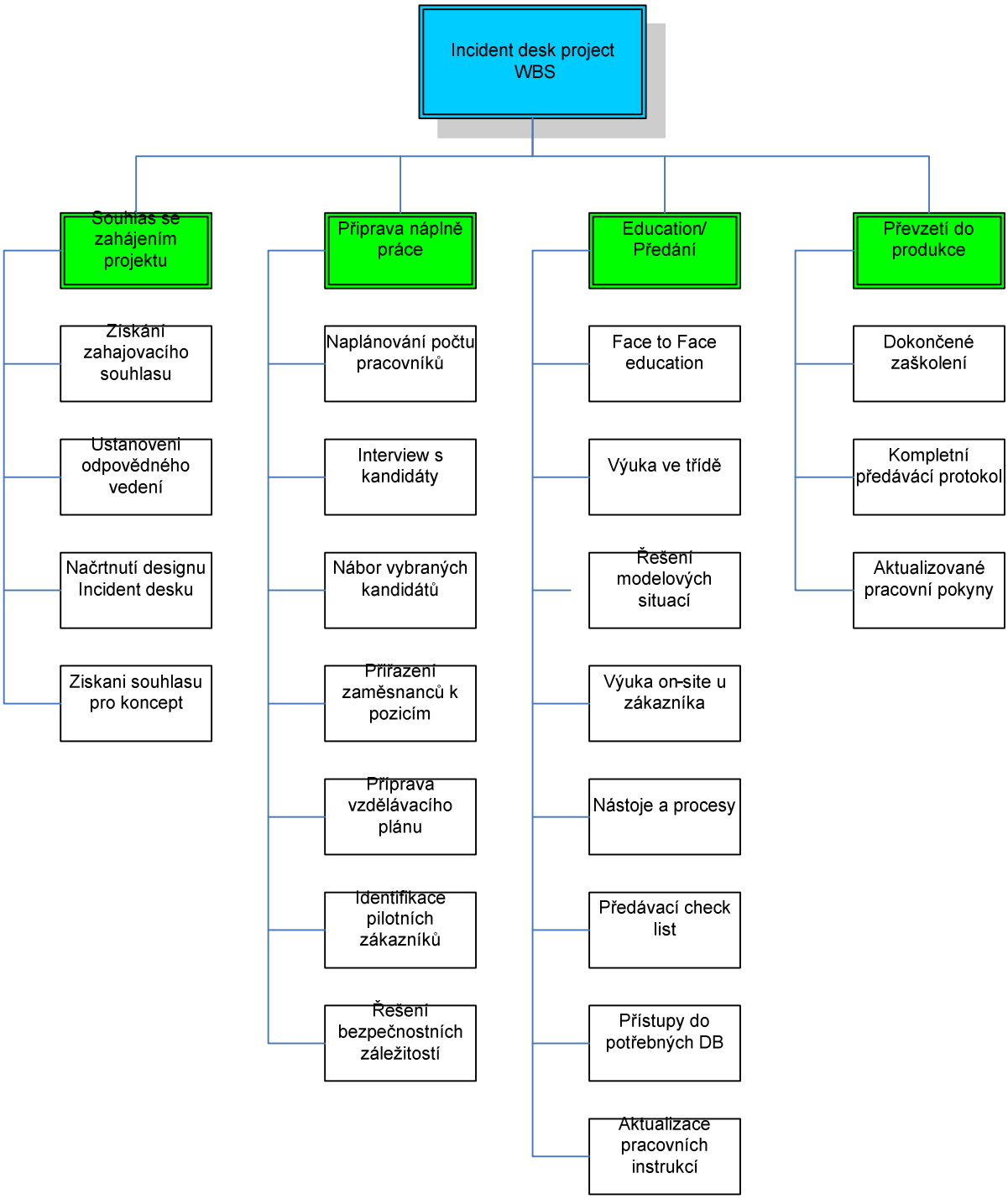
Výpočet kritické cesty:

Dle grafu a přiložené tabulky vede kritická cesta těmito uzly: 9, 7, 6, 5, 4, 2, 1 = 20+40+60+80+140+120 = 460

Vyhodnocení:

Po výpočtu všech potřebných veličin a dosazení do tabulky zjišťujeme, že kritická cesta vede uzly 1, 2, 4, 5, 6, 7 a 9 a to v trvání 460dnů. Díky 10 denní možné prodlevě se začátkem projektu, není zde task s nulovou rezervou času, rezervy u jednotlivých kroků se pohybují v rozpětí od 10 do 60 dnů. Realizace celého projektu od jeho přípravy po zavedení ostrého provozu zabere cca. 22 měsíců.

4.9 Analýza potřebných činností



Obrázek 10: WBS projektu

Návrh podrobného plánu pro zřízení Incident desku.

Dekomposice struktury činností na první rozlišovací úrovni (1.úroveň členění WBS – Work Breakdown Structure):

1.Souhlas se zahájením projektu
2.Příprava náplně práce
3.Education/ Předání
4.Převzetí do produkce
5.Ukončení projektu

Dekomposice struktury činností na druhé rozlišovací úrovni (2.úroveň členění WBS) projektu:

1. Souhlas se zahájením projektu

1.1.Získání zahajovacího souhlasu od TOP managementu
1.2.Ustanovení odpovědného vedení projektu
1.3.Sestavení plánu komunikace v projektu
1.4. Návrh conceptu Incident management desku
1.5. odsouhlasení conceptu TOP managementem

2. Příprava náplně práce

2.1. Stanovení potřebného počtu pracovníků
2.2. Uskutečnění interview s vybranými kandidáty
2.3. Nábor vybraných kandidátů
2.4. Uvedení vybraných kandidátů do funkce
2.5. Příprava vzdělávacích plánů
2.6. Identifikace pilotních zákazníků
2.7. Řešení security otázek

3. Education/ Předání

3.1.Face to Face education – skilltransfer od zkušených pracovníků
3.2. Classroom education – absolvování potřebných kurzů a školení
3.3. Řešení modelových situací – simulace reálného provozu

3.4. Výuka on-site u zákazníka – seznámení se se zákaznickým prostředím a jeho požadavky
3.5. Nástroje a procesy – vybavení se a zaškolení k práci s potřebnými tooly a seznámení se s procesy k jednotlivým zákazníkům.
3.6. Vytvoření předávacího check-listu – protokolu, trackovaní současného stavu fáze předáváaní a zaškolování.
3.7. Zajištění potřebných přístupů SW/HW (budovy, místnosti, databáze atd..)
3.8. Aktualizace working instructions (pracovních předpisů) a SSOW (dokument o kompletní náplni pozice Incident managementu)
3.9. Pilotní paralelní produkce

4. Převzetí do produkce

4.1. Ukončené veškeré plánované vzdělávací programy, ukončený skilltransfer
4.2. Vyplněný a uzavřený check-list (předávací protokol), odsouhalsený oběma stranami (předávající a přebírající)
4.3. Plně aktualizované working instructions (pracovních předpisů) a SSOW (dokument o kompletní náplni pozice Incident managementu), odosuhalseno a podepsáno zodpovědnými zástupci z řad managementu.
4.4. Ukonečena a vyhodnocena paralelní produkce, případné nedostatky a připomínky zaimplementované do finálních dokumetů
4.5. Schválení ukončení předávací fáze a odsouhlasení k zahájení ostrého provozu

5. Ukončení projektu

5.1. Příprava závěrečné zprávy
5.2. Kontrola dokladového zajištění + archivace
programové licence
osvědčení z kurzu
presence z instruktáže
přejímacích protokolů
inventárních záznamů
záznamů z porad projektového týmu
projektové dokumentace

5.3.Projednání a schválení závěrečné zprávy projektu
5.4.Ukončovací mítink

4.10 Zhodnocení návrhu

Ve zhodnocení mého návrhu bych nejdříve započal hodnocením kladných dopadů a vlivů při aplikaci modelu na reálný provoz a tím vlastně i odpovězení na otázku, zali bylo dosaženo cílů, které byly stanoveny v úvodu této práce. Hodonocení kladných dopadů rozdělím na dvě části a to na zhodnocení z pohledu provozovatele, podnikatele a na zhodnocení ze stran uživatele, zákazníka.

Stanovení počtu pracovníků na pokrytí uvažovaného Incident desku

- Plánovaná pracovní doba Incident desku je 7/24/365
- Jsou plánovány 12h pracovní směny v časových intervalech 06am-18pm, 18pm–06a.m
- Pokrytí směn je plánován na 2FTE/day a 1FTE/night (minimální pokrytí alespoň 1FTE/shift)
- Koeficient pro pokrytí absencí je 0.8

Projdeme si postupně cíle a jak se po implementaci Incident desku podílejí jendotlivě na přínosech pro organizaci.

- Postupné nahrazení služby Manager on Duty

Vzhledem k působení Incident desku dle specifikace v rámcí pokrytí 7/24/365 je takto zajištěno pokrytí služeb ohledně vyskytnuvších se incidentů v jakoukoliv denní či noční hodinu, roční období, státní svátek či situaci. Služba MoD (manager on duty) zajišťuje včasnou reakci na incidenty vyskytnuvší se v organizaci i mimo standardní pracovní dobu či o víkendech, státních svátcích a pod. Jelikož tato forma služby vyžaduje velké nároky na znalost prostředí organizace, podpůrných týmů a procesů, případně externích skupin podpory, je vykonávána povětšinou řídícími pracovníky minimálně ze středního, ale spíše z vyššího managementu, neboť s touto službou přicházejí zároveň i rozhodovací pravomoce a pravomoc řidit veškeré činnosti podílející se na vyřešení

incidentu. Z toho vyplývá, že finanční stránka této služby není zrovna zanedbatelná, navíc se musí vzít v potaz, že klade další zvýšené nároky na již tak dost psychycky vytížené managery, kteří namísto odpočinku musí vykonávat další služby nad rámec svých běžných povinností a to kdykoli. Z toho vyplývá, že převedení této služby na Incident desk je logickým krokem, neb zde pracující odborníci jsou zaměření a vycvičeni právě ve zvládání takovýchto situací a to v rámci své standartní mzdy a pracovní doby, což vede nejen ke úsporám mzdovým, ale samozřejmě se vrací zpět organizaci i ve formě odpočinutějších managerů připravených podávat maximální výkony ve svých řídících činnostech.

- Vedení denních service status callů pro určeného zákazníka a správa a údržba dat na Servis Management internet portálu

Správa SM portálu je jednou z nejdůležitějších čnnosti ohledně komunikace o právě probíhajích incidentech a stavu v jakém se nacházejí. Toto umožňuje jasný přehled o situaci ve firmě, o možnách výpadcích systémů, případně pokud je to možné i informaci o času potřebném k vyřešení nastálé situace. Dalšími doplňkovými infomacemi může být informaco dopadu na služby, kdo daný incident řeší, případně kontaktní osoba pro poskytnutí informací o posledním vývoji situace. Důležitá je dostupnost takovéhoto portálu pro všechny řídíci pracovníky společnosti, kteří v případě nastálých problémů moho zde nejprve zkontorlovat, zda je toto již v řešení, či je-li třeba toto nahlásit jako nový incident, připadně se může obrátit na zde uvedenou osobu o bližší informace o probíhajícím incident, nebo naopak s informacemi, které mohou být použity k rychlejší nápravě situace.

Vedení pravidelných service status callů, patří k dalším důležitým informačním nástrojům a částečně jsou i nástrojem proaktivní politiky, kde se ná základě projednávaných informací dají dále predikovat další chování určitých systému a na jejich základě přijmout preventivní opatření. Vetšinou se jedná o výskyt četností jednoho a toho samého incidentu, připadně různých událostí, ketré se vyřeší samy bez jakéhokoliv zásahu. Tyto cally jsou většinou na denní bázi a slouží k informování středního a vyššího managemenu zejména o:

- Probíhajících incidentech
- O incidentech za posledních 24h

- Backlogu z minulých callů
- Otevřených Problem ticketů na základě Incidentů
- Různých podnětech či požadavcích na zvýšení kvality servisu

Jak již bylo, informace z těchto callů jsou vstupem pro proaktivní politiku organizace a jako takové dokaží ve svém výsledku, pokud jsou správně využity, ušetřit organizaci nemalé sumy prostředků do budoucna. Neboť ztráty třeba v důsledku 1h výpadku důležitých obchodních(E-Commerce) systémů se mohou dle velikosti a zaměření organizce pohybovat od několika stovek až po milionové či destimilionové (a více) částky v národních měnách.

- Řízení a vedení řešení všech incidentů s vysokou prioritou (Severity1 a Major incident), působí jako counterpart pro SDM/DPE/AITA and DSL + IT specialisty přes všechny spravované zákazníky

Čimmost tvořící tzv. daily bread, neboli hlavní náplň činnosti Incident desku – zodpovědnost za celý životní cyklus incidentu, od nahlášení přes fázi řešení až po uzavření incidentu. Indident manager jako takový nakládá převážně s informacemi, předává je zainteresovaým stranám v půběhu incidntu, dohlíží na nakládání s nimi, spolus dohledem nad vývojem situce, z tohoto provádí online reporting zůčastněným stranám, inicijuje všechny potřebné činnosti a řidí veškerý průběh událostí tak, aby minimalizoval dopad incidentu na chod organizace, případně na její zákazníky. Jak již bylo naznačeno o odstavec výše, každá uspořená hodina, či dokonce minuta z doby účinnosti incidentu může ve svém důsledku znamenat úspory významných finnačních hodnot, vedle dalších, jako je stráta důvěry, dobrého jména společnosti, ztráta zákazníků atd, které jsou ve svých důsledcích minimálně na stejné úrovni jako ony dopady finanční a pro společnost mohou být až životně důležité.

- Office time pro Incident desk je 24/7/365 (nepřetržitý provoz) ve 12h směnách

Ve výše uvedeném projektu jsem navrhl osazení Incident desku s ohledem na platnou legislativu v ČR, tak aby bylo možno zajistit nepřerušený servis. V dnešní době

globalize a rozvoje elektronických služeb v nepřeberném množství odvětví se již nemůže uspokojit s poskytováním našich služeb pouze od pondělí do pátku a 8h denně, jak bylo zvykem dříve. Dnes s možností dosažení našeho businessu ze zemí s rozdílnými časovými pásy, či zvyklostmi, musíme učinit náš business dostupný a hlavně funkční defacto neustále, neboť každá ztracená hodina, nebo dokonce i minuta může znamenat ztrátu potenciálního zákazníka, který nemá problém tzv. „zajít“ ke konkurenci, když mu toto dnes zabere cca 1min jeho času. Navíc pokud hovoříme o elektronických transakcích a E-Commerci, nesmíme opomenout bankovní ústavy, kde již dávno nekolují peníze fyzické, ale elektronické a tyto toky jsou defacto nepřetržitým proudem toků dat v řádech miliard a nebudu přehánět, pokud řeknu, že každou minutu. A pro tyto organize je zajištění provozu těchto systémů životně důležité, neboť zde každý výpadek, či chyba, je okamžitě odražena ve výši astronomických čisel.

- Zajištění maximální customer satisfaction v rámci kontraktovaných SLA

Zajištěním všech předchozích cílů dosáhneme tohoto posledního cíle, který defacto definuje úroveň spokojenosti zákazníků (ať už interních, nebo externích) s poskytovanými službami. Zde se střetávají dva poheldy na věc. První je pohled zákazníka – který chce za své peníze dostat kontraktované služby v patřičném množství a kvalitě – pokud dokáže on díky našim službám uspokojovat potřeby svých zákazníků a rozvíjet se, je zákazník spokojený, což dále vede k prodloužení kontraktů, či ústí v posílení důvěry a vzájemných vztahů, případně možnosti mimořádných odměn atd. Z pohledu poskytovatele služby je to pohled podobný, maximální uspokojení zákaznických požadavků vede k tvorbě dobrého jména, finančního zabezpečení a dobré pozice pro další vyjednávání při prodlužování kontraktů a pod. Opačný případ defacto neguje předchozí a dochází ke strátě jména, hrazení finančních strát zákazníka a posléze jeho odchodem ke konkurenci.

Pokud tedy shrnu všechny předchozí body, které byly výchozím cílem projeku, a byly stanoveny s ohledem na hlavní cíl mé diplomové práce, při důsledné implementaci a následném vytvoření všech navazujících procesů tak, aby byl nejen Incident management ale i ostatní složky service managementu funkční, je toto jedním z nejdůležitějších implementovaných procesů v případě přenosu rizik na druhý subjek,

případně minimalizace dopadu incidentu v připadě zřízení Incident desku vlastními silami. Tímto můj projekt naplňuje zadaný cíl mé práce a to „návrh modelu Incident managementu pro organizace zabývající se elektronickým obchodováním, jakožto jednoho ze základních prvků zabezpečujících snižení rizik a ztrát způsobených výpadkem „bussiness crtitcal“ aplikací a infrastruktury.“ Pro názornost následující tabulka ukazuje případný možný dopad na příjmy TOP E-commerce společností .

Company	Revenue 2010 (mil $)	Revenue/měsíc (mil $)	Revenue/den (mil $)	Revenue/hod (mil $)
Costco.com	$71 422,00	$5 951,83	$198,39	$8,27
Dell.com	$52 902,00	$4 408,50	$146,95	$6,12
bestbuy.com	$49 694,00	$4 141,17	$138,04	$5,75
Amazon.com	$24 509,00	$2 042,42	$68,08	$2,84
Google	$23 650,00	$1 970,83	$65,69	$2,74
JCP.com	$17 556,00	$1 463,00	$48,77	$2,03
Gap.com	$14 197,00	$1 183,08	$39,44	$1,64
Liberty Media	$10 398,00	$866,50	$28,88	$1,20
Ebay	$8 727,00	$727,25	$24,24	$1,01
Yahoo	$6 460,00	$538,33	$17,94	$0,75

Tabulka 7: Přehled příjmů TOP společností z oblasti E-Commerce (zdroj: http://ceoworld.biz/ceo/2010/03/25/top-most-popular-e-commerce-e-business-or-online-retailer-websites-reviews a http://money.cnn.com/magazines/fortune/global500/2010/full_list/)

5. Závěr

Ve své práci jsem se pokusil poukazat na Incident managementu jako na významný moderní prostředek k mitigaci, predikci, avoidanci, či přesunu rizik na jiný subjekt. Jeho uzké provázání s managementem rizik je více než zřejmé, neboť tam kde nejsou rizika, nemá Incident management smysl, jelikož tam nemá žádnou živnou půdu ani opodstatnění. Z tohoto nám tedy vyplývá otázka, pro koho je vlastně Incident management vhodný? Je možno ho implementovat úplně všude, nebo jen tam, kde jsou firmy bohaté a každý dopad incidentu je vyčíslován ve vysokých částkách? Moje odpověď na tuto otázku je jasná, incident mamagement je výhodný všude tam, kde nám jde o zákazníka a úspěšný rozvoj naší firmy, což si myslím by mělo být náplní každého podnikání a cílem každého podnikatelského subjektu. Takže Incident management může být stejně výhodný jak pro nadnárodní konglomerát firem, tak i pro malou regionální firmičku, či dokonce i pro osobu samostaně výdělečně činnou, která je sama sobě šéfem i zaměstanancem. Kde se bude lišit přístup těchto organizačních protipólů je způsob implementace. Nadnárodní spoečnost nejsíše využije cestu outsourcingu těchto služeb, kdežto málá firmička, či dokonce jednotlivec toto zajistí někým z vlastních řad, ať už dedikovanou osobou, či v případě těch nejmenších sharovanou s nějakou další rolí. Neboť pokud se zamyslíme nad problémem hlouběji, dojdeme k otázce, co je vlastně Incident management sám o osbě? Je to něco, co musí být pojmenováno v rámci organizace? Kde musí být jedinec skupina lidí, či department, který má toto v názvu? Nebo je to způsob chování? Způsob, jakým je organizace schopna řešit problémy uvnitř své vlastní organizace s minimalizací dopadů a maximalizací spokojenosti svých zákazníků? Sobně zastávám názor, že je to způsob chování, který liší efektivní Incident management od neefektivního a jeden Incient manager může být vzhledem k implementaci efektivnější než celý dedikovaný Incident management department. Pokud se zamyslím, kdyže Incident management vznikl, určitě daleko před ITIL, či jiným systémem řízení. Už od nepaměti byly v každé firmě lidé, kteří tzv. „vědí“, vědí koho zavolat, pokud se stano toto, nebo tamto, jak se to vyřešilo minule a pod. Sytémy ITSM a defacto normy ISO a pod., pouze převedli tyto „best practices“ do jednotné formy, poskladali drobné úlomky a umístili je na jedno místo, kde mají posloužit případným zájemcům o ať už rozjetí nového, nebo zlepšení již rozjetého businessu, co

by neměo v jejich organizaci chybět a jak by to asi mohlo vypadat, nebo spíš co by nemělo chybět. ITIL sám o sobě slouží tedy jen jako rámec, neurčuje detaily a postupy, ty si každá organizace určuje sama dle jejího zaměření. Někdy vidíme snahy některých společností v rámi být tzv.“IN“ implemetovat co se kde šustne s vyhlídkou, že jakmile se všechno zavede, stanou se z nich TOP společnosti se spoustou certifikátů a atd. A někdy to bohužel vede k tomu, že se absolutně nevhodné rámce čehokoliv implemetují způsobem, že se firma ohýbá dle stanovených regulí, namísto aby se vybralo pouze jen to funkčí a to se implementovalo. Někdy se tak firma dostane do situace, kteríá paradoxně působí kontraproduktivně a nakonec to vede k záhubě společnosti, ať už vinou finančních náročností změn, které nejsou zdaleka vyváženy přínosy, nebo úplnou destrukcí organizační struktury, které v konečeném výlsedku vede k roztavení firmy a totálnímu rozkladu portfólia poskytovaných služeb zároveň s propadem v jejich kvalitě. Proto Incident mamagement, přestoře je přínosný, jak jsem již uvedl výše, defacto pro každého, i při jeho implementaci je potřeba toto přizpůsobit požadavkům konkrétní společnosti, neboť není důležité kolik lidí se o vaše incidenty stará, ale jak jsou efektivní. Takže ne základě předchozího bych si dovolil odpověď na otázku, pro koho Incident managemnt vůbec je odpovědět takto: „Incident mamagement je vhodný pro každého, za podmínek vhodné implemetace dané potřebami a rozsahem dané společnosti pro dosažení maximální efektivity.“ Proto nebojme se Incident mamagementu, není to vždy že musíte mít skupinu lidí, nebo si platit externí organizaci, která vám bude tyto služby poskytovat. Stačí být seznámen alespoň se základy Incident mamagementu jako takovými a pak se sami rozhodnete, co implementujete a jakým způsobem, hlavně efektivně. Pak bude firma vždy připravena čelit nenadálým událostem v maximální možné míře, ať již formou reakce, či prevence a využít toto jako svou konkurenční výhodu při boji o pozici na trhu.

Použité zdroje

1. CASE, G. DUMOULIN, T. SPALDING, G. DISSANAYAKE, A. *Service Management Strategies that Work*, Van Haren Publishing, 2007, ISBN 9789087530488

2. CARTLIDGE, A. HANNA, A. RUDD, C. MACFARLANE, I. WINDEBANK, J. RANCE, S. *An Intorductory Overview of ITIL V3*, itSMF Ltd, 2007, ISBN 0-9551245-81

3. DOSEDĚL,T. *Počítačová bezpečnost a ochrana dat.* 1. vydání. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1

4. DRDLA, M., RAIS, K.: *Řízení změn ve firmě – reengineering: jak vybudovat úspěšnou firmu.* 1. vyd. Praha: Computer Press, 2001. 144 s.

5. Editorial Board, IT *Service Management Global Best Practices*, Van Haren Publishing, 2008, ISBN 978-9087531003

6. EVANS, I. MACFARLANE, I. *A Dictionary of IT Service Management*, Van Haren Publishing, 2006, ISBN 978-0952470656

7. FRY, M. *Building an ITIL-based Service Management Department*, TSO, 2008, ISBN 978-0113310968

8. JONG,A. KOLTHOF, A. PIEPER, M. TJASSING, R. VEEN, A. VERHEIJEN, T. *Foundations of IT Service Management based on ITIL V3*, Van Haren Publishing, 2007, ISBN 978-9087530570

9. KILLCRECE, G. *Incident management* [online] Dostupné z: https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/incident/223-BSI.html

10. KOTLER, P. *Marketing management.* 1. vydání, Praha: Grada, 2007. 788 s. ISBN 978-80-247-1359-5

11. OGC, *Management of Risk Pocketbook*, TSO, 2007, ISBN 978-0113310661

12. OGC, *Key Element Guide Service Operation*, TSO, 2008, ISBN 978-0113311187

13. OGC, *Service Support*, TSO, 2000, ISBN 978-0113300150

14. OGC, *Service Operation*, TSO, 2007, ISBN 978-0113310463

15. PUŽMANOVÁ, R. *Moderní komunikační sítě od A do Z.* 2. aktualizované vydání. Brno: Computer Presss, 2006. 430s. ISBN 80-251-1278-0

16. RAIS,K., SMEJKAL,V.: *Řízení rizik ve firmách a jiných organizacích*. 3. vydání. Praha, GRADA. 2009, 360 str., ISBN 978-80-247-3051-6

17. SODOMKA,P. *Informační systémy v podnikové praxi*. 2.aktualiozované vydání. Brno: Computer Press, 2010. 499s. ISBN 978-80-251-2878-7

18. STERNECKER, A.B*. Critical Incident management* [online] Dostupné z: http://flylib.com/books/en/3.221.1.77/1/

19. VOŘÍŠEK, J. *Principy a modely řízení podnikové informatiky*. 1. vydání. Praha: Oeconomica, 2008. 446 s. ISBN 978-80-245-1440-6

20. *CobiT* [online] Dostupné z: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/CobiT.aspx

21. *CMMI* [online] Dostupné z: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/CMMI.aspx

22. *ISO 27001* [online] Dostupné z: http://www.mbk.cz/iso-27001

23. *IT Incident management* [online] Dostupné z: http://www.sun.com/emrkt/sunspectrum/Incd.Mgmt_Wht_ppr_5.22.pdf

24. *Incident management* [online] Dostupné z: http://www.itsmportal.cz/cs/ITIL/Discipliny-ITSM-dle-ITIL-/Incident-Management.alej

25. *ITIL* [online] Dostupné z: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/ITIL.aspx

26. *Lean* [online] Dostupné z: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/Lean.aspx

27. *Managing risk in e-commerce* [online] Dostupné z: http://www.businesslink.gov.uk/bdotg/action/layer?r.i=1075386132&r.l1=1073861197&r.l2=1073866263&r.l3=1075386080&r.s=sc&r.t=RESOURCES&topicId=1075386080

28. *Six Sigma* [online] Dostupné z: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/SixSigma.aspx

Seznam příloh:

I. Historie obchodu a E-Commerce
II. Incident management process flow
III. Další zdroje informací k tématu

Příloha I: Historie obchodu a E-Commerce

1.1 Historie obchodu a peněz

Ve velmi dávné historii, na počátku samého obchodování, když ještě nebyly vynalezeny peníze, se obchodovalo ve své nejprimitivnější formě tzv. barteru, což je přímá výměna zboží a služeb za jiné zboží a služby. Postupem času však toto obchodování bylo více a více komplikovanější, a tak byl barter nahrazen různými formami peněz. Prvními penězi se staly fyzické komodity, jejichž hodnota byla velmi dobře známa (kukuřice, sůl, zlato). V důsledku několika žádoucích vlastností, jako byla například přenositelnost či dělitelnost, se stalo zlato a stříbro nejužívanějším platidlem a to asi do začátku 19. století. [1, 2]

Dalším krokem ve vývoji peněz bylo používání mincí a papírových bankovek, které již známe z vlastní zkušenosti. Důvěryhodnost peněžního systému byla garantována místní, národní či mezinárodní bankou, která kontrolovala tisk nových bankovek a ražbu nových mincí. Platba v hotovosti pomocí mincí a bankovek se stala a stále je nejpoužívanější formou směny peněz. V posledních letech však pozorujeme trend, kdy lidé placení v hotovosti stále více omezují, což je způsobeno především díky tomu, že lidé již nechtějí shromažďovat u sebe větší sumy peněz, ale mají je raději na svých peněžních kontech, kde se úročí a dále pak díky větší bezpečnosti svých finančních prostředků (když mi někdo ukradne platební kartu na PIN, ještě to neznamená, že přicházím o peníze, protože zloděj PIN nezná, ale když mi někdo ukradne peněženku s penězi, tak už se s nimi nesetkám). [1, 2]

Vznikly šeky, platební poukázky, "plastikové" peníze a "opravdové" peníze se přesunovaly hlavně mezi bankami po bezpečných finančních sítích, začalo se obchodovat přes telefon, mail, kdy se nakupující ani prodávající navzájem neviděli, a tak nebylo možné ověřit zda se nakupující či prodávající nepokouší o podvod. Peníze se tedy pomalu ale jistě začínají více a více přemísťovat elektronicky (nejvíce je to samozřejmě patrno v nejrozvinutějších částech světa a zemích, které udávají tempo celosvětového obchodu a které nejvíce ovlivňují finanční trhy atd.). [1, 2]

1.2 Historie E-commerce

Elektronická komerce (e-commerce), EPS a elektronický obchod pomocí Internetu je mladý, nedobře definovaný ale velmi perspektivní a dynamicky se rozvíjející obor. Velké organizace používají elektronickou komerci již nějaký čas k provádění svých vlastních transakcí mezi sebou. Přitom vlastní **Elektronická výměna dat (EDI)** na soukromých počítačových sítích začala již v šedesátých letech. Přibližně stejně dlouho používají banky specializované sítě pro **Elektronický transfer peněz (EFT)**.
Na vzniku a rozvoji elektronické komerce se největší mírou podílela velká popularita Internetu. Díky tomu, že jej stále více a více firem používá ke své činnosti, se na Internetu rozšiřují možnosti elektronického obchodování mezi firmami a elektronická komerce se tak stává zcela běžnou součástí obchodu. [1, 2]

Pro mnoho lidí elektronická komerce znamená nákup či prodej výrobků a služeb přes Internet. To je však pouze jedním z mnoha aspektů elektronické komerce. Ta se od svých počátků týkala řízení nákupních a prodejních transakcí a následných převodů peněžních prostředků s využitím počítačových sítí. Nyní se však rozvinula natolik, že zahrnuje nákup a prodej nových komodit, jako jsou například elektronické informace. Současná elektronická komerce umožňuje provádění zcela nových typů transakcí přes počítačové sítě, které nemají svoji obdobu v reálném světě. [1, 2]

Elektronická komerce původně spočívala v transakcích mezi velkými korporacemi, bankami a jinými finančními institucemi. Právě využití Internetu jako prostředku k přenosu elektronické komerce ke koncovému spotřebiteli, vedlo ke změně pohledu na věc.
Internet rovněž způsobil vzestupný rozvoj průmyslové elektronické komerce, která se rozvíjí rychleji než kdy dříve. Malé firmy zjišťují, že své obchody mohou provádět on-line právě tak, jako jejich větší konkurenti, s využitím Internetu a elektronického obchodování lze významně snížit náklady a přispět tak k vyšší efektivitě. [1, 2]

Položíme-li si otázku *"Co je elektronická komerce?"*, musíme si nejprve uvědomit, z čeho se skládá tradiční komerce. Tradiční komerce zahrnuje více než jen prodej předmětu a následnou platbu. Prodejní cyklus bez využití elektronické komerce má typicky několik složek - firmy navrhují a vyrábějí nové výrobky, umisťují je na trhy,

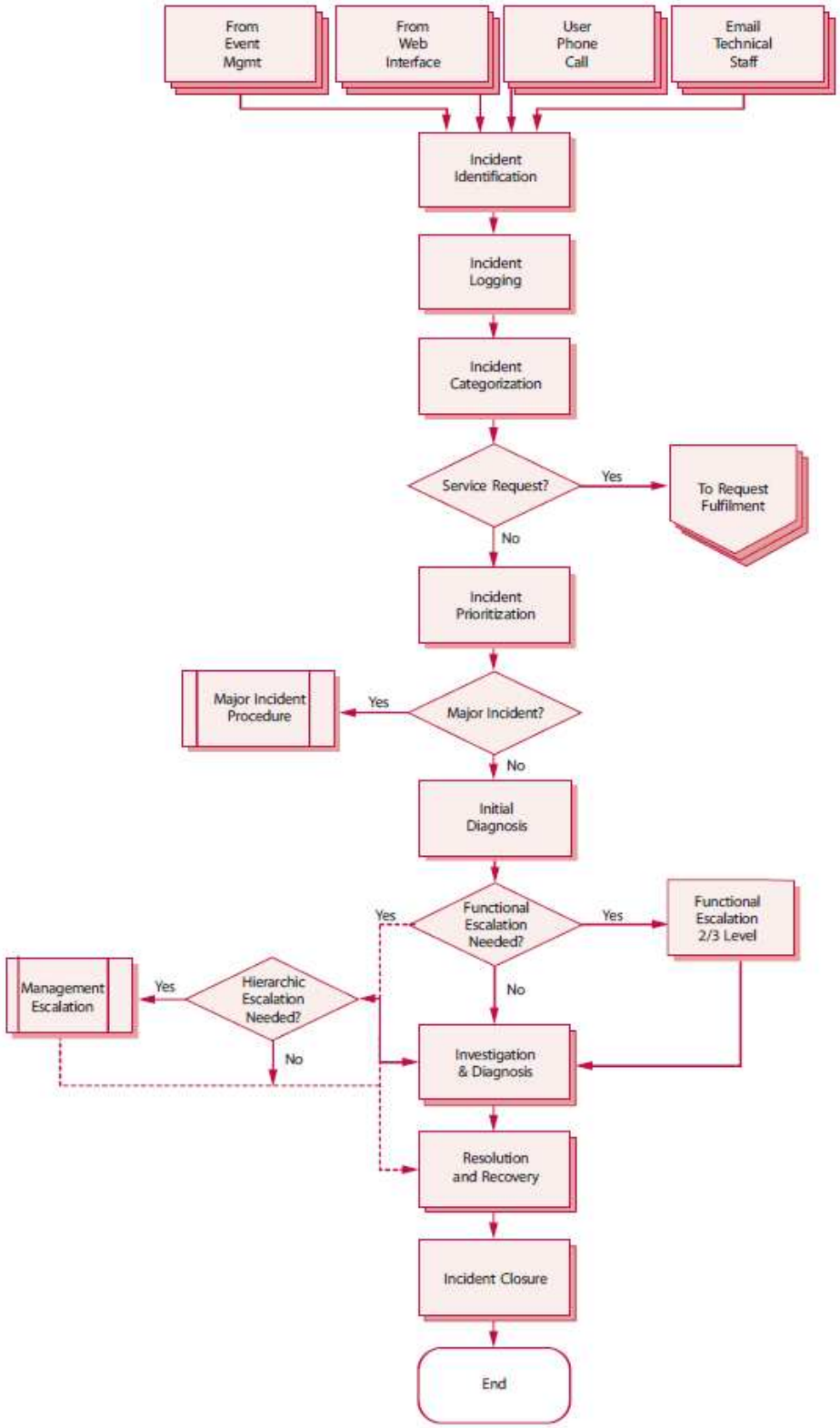
distribuují je a poskytují podporu zákazníkům. Uspokojováním potřeb trhu dosahují příjmů.

Zákazníci však musí nejprve rozpoznat potřebu něčeho, ať už je to fyzický produkt, služba nebo informace. Předtím, než skutečně nakoupí, hledají informace o tomto produktu nebo službě, místo prodeje a porovnávají varianty, které nalezli (např. ceny, pověst firmy, služby…) Prodejní cyklus vůbec nekončí pouhým dodáním výrobku - měla by následovat podpora zákazníkovi, ze které plyne užitek oběma stranám: zákazníci dostanou fungující výrobek a dodavatelé se dozvídají o potřebách trhu. Mezitím banky a finanční instituce provádějí převod peněžních prostředků mezi prodávajícím a kupujícím, ať už jsou to individuální spotřebitelé nebo velké mezinárodní korporace. Elektronickou komercí pak můžeme chápat systém, který obsahuje nejen transakce realizující nákup či prodej zboží a služeb, které slouží k přímé tvorbě příjmů, ale i transakce, které podporují produkci příjmů. Typickým příkladem může být vytváření poptávky po daném zboží či službě nebo podpora prodeje a služby zákazníkům usnadňující komunikaci mezi obchodními partnery.

Elektronická komerce je postavena na výhodách a struktuře tradiční komerce s přidáním flexibility, kterou poskytují elektronické sítě. Usnadňuje různým skupinám spolupráci, řeší rychlou výměnu informací, odstraňuje fyzická omezení v důsledku čehož mohou například počítačové systémy na Internetu poskytovat podporu zákazníkům 24 hodin denně nebo přijímat a vyřizovat objednávky na výrobky či služby kdykoli a odkudkoli. Elektronická komerce zkrátka umožňuje vzniknout novým formám podnikání. Umožňuje firmám uzavřít prodejny, snížit potřebné zásoby a distribuovat výrobky pomocí Internetu.

Jako příklad si uveďme firmu Amazon.com se sídlem v Seattle ve státě Washington prodávající knihy. Tato firma nemá fyzické obchody, prodává všechny své knihy přes Internet a koordinuje dodávky knih přímo s vydavateli, takže nemusí udržovat žádné zásoby. [1, 2]

Příloha II: Incident management process flow



Obrázek 11: Incident management process flow based on ITIL (**zdroj**: http://www.securityprocedure.com/incident-management-process-flow-templates)

Příloha III:

Použité zdroje příloh:

1. FRANCU, M. *Internet pro podnikatele*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-623-3.

2. /online/ Historie a současnost elektronického bankovnictví a e-komerce. Dostupné na http://www.fi.muni.cz/usr/jkucera/pv109/2001/xcodl.html

Další zdroje:

FRIMMEL, M. *Elektronický obchod:právní úprava*. 1.vyd. Prospektrum. Praha. 2002. 321 s. ISBN 80-7175-114-6

GRUBLOVÁ, E. aj. *Internetová ekonomika*, 1. vyd. Ostrava: Repronis. 2002. ISBN 80-7329-006-6.

JAMES, L. *Phishing bez záhad*. 1.vyd. Grada Publishing. Praha. 2007. 281 s. ISBN 978-80-247-1766

KOSIUR, D. *Principy a praxe elektronické komerce*. Computer Press. Brno. 2000.

MÁČE, M. *Platební styk-klasický a elektronický*. 1.vyd. Grada Publishing. Praha. 2006. 220 s. ISBN 80-247-1725-5

MATYÁŠ, V. a KRHOVJÁK, J. *Autentizace elektronických transakcí a autorizace dat i uživatelů*. Masarykova univerzita. Brno. 2008.

PŘÁDKA, M. a KALA, J. *Elektronické bankovnictví:rady a tipy*. 1.vyd. Computer Press. Praha. 2000. 166 s. ISBN 80-7226-328-5

SEDLÁČEK, J. *E-komerce:internetový a mobil marketing od A do Z.* 1.vyd. BEN - technická literatura. Praha. 2006. 351 s. ISBN 80-7300-195-0

TONDR, L. *Podnikáme s Internetem*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-729-9.

VRABEC, V. a WINTER, J. *Internet, podnikatelská příležitost nebo hrozba?*, 1. vyd. Praha. Management Press. 2000. ISBN 80-7261-026-0.

WOODS, A. a WILLIAM W. *Internetová tržiště B2B pro 21.století*. 1.vyd. P.Wimmer. Unhošť. 2004. 277 s. ISBN 80-239-3899-1

FORD, W., BAUM, M.S. *Secure Electronic Commerce*, Prentice Hall, 1998

FRANCU, M. *Internet pro podnikatele*, 1. vyd. Praha: Computer Press. 2002. ISBN 80-7226-623-3.

FRIMMEL, M. *Elektronický obchod:právní úprava*. 1.vyd. Prospektrum. Praha. 2002. 321 s. ISBN 80-7175-114-6

GHOSH, A. K. *E-commerce security*, John Wiley, 1998

GRUBLOVÁ, E. aj. *Internetová ekonomika*, 1. vyd. Ostrava: Repronis. 2002. ISBN 80-7329-006-6.

HANÁČEK, P. *Security of Electronic Money*, in SOFSEM ´99, Lecture Notes No. 1521, Spinger-Verlag, 1998, 107-121

KOSIUR, D. *Principy a praxe elektronické komerce*. Computer Press. Brno. 2000.

LACOSTE, G. *SEMPER: A Security Framework for the Global Electronic Marketplace*, SEMPER document 431LG042, IBM France, August 1996

MÁČE, M. *Platební styk-klasický a elektronický*. 1.vyd. Grada Publishing. Praha. 2006. 220 s. ISBN 80-247-1725-5

MATYÁŠ, V. a KRHOVJÁK, J. *Autentizace elektronických transakcí a autorizace dat i uživatelů*. Masarykova univerzita. Brno. 2008.

PŘÁDKA, M. a KALA, J. *Elektronické bankovnictví:rady a tipy*. 1.vyd. Computer Press. Praha. 2000. 166 s. ISBN 80-7226-328-5

RUEPPEL, R. *Secure Banking over Internet: Recommendations from European Committe for Banking Standards*, ERCIM NEWS, 30, July 1997

SEDLÁČEK, J. *E-komerce:internetový a mobil marketing od A do Z.* 1.vyd. BEN - technická literatura. Praha. 2006. 351 s. ISBN 80-7300-195-0

SENDROVIC, I. *Security of Electronic Money*, Report by the Committe on Payment and Settlement Systems and the Group of Computer Experts of Central Banks of Group of Ten Countries (G-10), Basilej, ISBN 92-9131-119-7, 1996

SCHLOSSBERGER, O. a HOZÁK, L. *Elektronické platební prostředky*. 1.vyd. Bankovní institut. Praha. 2005. 144 s. ISBN 80-7265-073-4

VRABEC, V. a WINTER, J. *Internet, podnikatelská příležitost nebo hrozba?*, 1. vyd. Praha. Management Press. 2000. ISBN 80-7261-026-0.

WAIDNER, M. *Open Issues in Secure Electronic Commerce*, in Final report of the ACTS Project AC026, SEMPER, 1998

WOODS, A. a WILLIAM W. *Internetová tržiště B2B pro 21.století*. 1.vyd. P.Wimmer. Unhošť. 2004. 277 s. ISBN 80-239-3899-1

ZLATUŠKA, J. *Analýza podmínek pro přechod ČR k informační společnosti*, Zpráva pro Radu vlády ČR pro výzkum a vývoj, duben 1998

ZLATUŠKA, J. *Srovnání vybraných charakteristik přechodu k informační společnosti v ČR a ve světě*, Zpravodaj ÚVT MU, Masarykova universita Brno, prosinec 1998

DONELLY, J. H.,Jr. a kol.: *Management*. Praha: Grada Publishing, 1997. 821 s. ISBN 80-7169-422-3.

DRUCKER, P. F.: *Řízení v době velkých změn*. Praha: Management Press, 1998. 285 s. ISBN 80-8594-378-6.

FEHR, HANS-ULRICH.: *Total duality management*. Brno: Unis Publishing, 1995. 258s. ISBN 34-4617-135-5.

HAMMER, M.: *Agenda 21: Co musí každý podniku udělat pro úspěch v 21. století*. Překl. Hana Škapová. 1. vyd. Praha: Management Press, 2002. 62 s. ISBN 80-7261-074-0.

HAMMER, M., CHAMPY, J.: *Reengineering: radikální proměna firmy: manifest revoluce v podnikání*. 3. vyd. Praha: Management Press, 2000. 212 s. ISBN 80-7261-028-7.

HRON, J., TICHÁ, I., DOHNAL, J.: *Strategické řízení.* Praha: Česká zemědělská univerzita – Provozně ekonomická fakulta, 2000. 266 s. ISBN 80- 213-0625-4.

JANEČEK, Z.: Zajišťování jakosti. Plzeň: Západočeská univerzita, 2001. 94 s. ISBN 80-7082-807-2.

KOPČAJ,A.: *Košatění bohatství.* Ostrava: Silma´90, 1997. 186s. ISBN 80-9023-580-8 .

KOPČAJ, A.: *Řízení proudu změn aneb všedním způsobem nevšední rozvoj firmy*. Ostrava: Silma ´90, 1999. 298 s. ISBN 80-9023-581-6.

KOTTER, J. P.: *Vedení procesu změny*. Praha: Management Press, 2000. 190 s. ISBN 80-7261-015-5.

MAKOVEC, J.: *Základy řízení výroby.* 1. vyd. Praha: VŠE, 1997. 98 s. ISBN 80-7079-110-1.

MALÝ, M., DĚDINA, J.: *Organizační architektura*. Praha: Victoria Publishing a.s., 1996. 170s. ISBN 80-7178-064-1.

NENADÁL, J. a kol.:*Moderní systémy řízení jakosti.* Praha: Management Press, 2002. 282 s. ISBN 80-726-1071-6.

PALÁN, J, F., KOTVOVÁ, H.: *Management organizační změny*. 1. vyd. Praha: Credit, 1998. 142 s. ISBN 80-213-0377-8.

PALÁN, J. a kol.: *Řízení změn*. 1. vyd. Praha: Credit, 2002. 256 s. ISBN 80-213-0893-1.

ROBSON, M., ULLAH, P.: *Praktická příručka podnikového reengineeringu.* Praha: Management Press, 1998. 178 s. ISBN 80-85943-64-6.

ŘEPA, V.: *Podnikové procesy. Procesní řízení a modelování*. Praha: Grada Publishing, 2006. 265 s. ISBN 80-247-1281-4.

TOMAN, M.: *Řízení změn.* 1. vyd. Praha: Alfa Publishing, 2005. 148 s. ISBN 80-86851-13-3.

TRUNEČEK, J.: *Systémy podnikového řízení ve společnosti znalostí*. Praha: VŠE, 1999. 184 s. ISBN 80-7079-083-0.

VACULÍK, J.: *Řízení změn I. Díl, Vybrané kapitoly – základy a postupy*. 1. vyd. Pardubice: Univerzita Pardubice, 2006. 141 s. ISBN 80-7194-833-0.

VACULÍK, J., BERKA, A., KUBĚNKA, M.: *Řízení změn II. Díl, Implementace změn*. 1.vyd., Pardubice: Univerzita Pardubice, 2006. 89 s. ISBN 80-7194-834-9.

VEBER. J.: *Management kvality od ISO 9000 k TQM.* Nakladatelství Máchova kraje, 1997. 247 s. ISBN 80-9017-305-5.

VEBER. J.: *Management II*. Praha: VŠE, 1998. 168 s. ISBN 80-7079-406-2.

VEBER. *J.: Řízení jakosti a ochrana spotřebitele*. Praha: Grada, 2007. 201 s. ISBN 978-80-247-1782-1.

VODÁČEK, L., VODÁČKOVÁ, O.: *Management – Teorie a praxe v informační společnosti*. Praha: Management Press, 2001. 314 s. ISBN 80-7261-041-4.

MC CORMACK, M.H. *Co vás nenaučí na Harwardu aneb Jak úspěšně podnikat*. Prostor Praha 1992. Str.279. ISBN 80-85190-14-1

MOLNÁR, Z. *Efektivnost informačních systémů*. Grada. Praha 2001.179s. ISBN 80-247-0087-5

JOHNSON,G., SCHLOES, K.: *Cesty k úspěšnému podniku*. Computer Press, Praha 2000. Str. 803. ISBN 80-7226-220-3

KAPLAN, R.S. , NORTON,D.P. : *Balanced Scorecard. Strategický systém měření výkonnosti podniku*. Management Press, Praha 2007. Str. 270**.** ISBN 978-80-7261-177-5

PETERS,T.,WATERMAN,R.H.: *Hledání dokonalosti - Poučení z nejlépe vedených amerických společností.* Svoboda – Libertas. Praha 1992. Str. 294. ISBN 80-205-0313-7

DĚDINA, J.: *Podnikové organizační struktury. Teorie a praxe*. Victoria Publishing Praha,1996. Str.117. ISBN 80-7187-029-3

KOTTER, J.P.: *Vedení procesu změn*. Management Press, Praha 2000.str. 190. ISBN 978-80-7261-015-0